GIBSON DUNN

2019 Year-End Sanctions Update

Client Alert | January 23, 2020

Between claims of “financial carpet bombing” and dire warnings regarding the “weaponization” of the U.S. dollar, it was difficult to avoid hyperbole when describing the use of economic sanctions in 2019. Sanctions promulgated by the U.S. Department of the Treasury’s Office of Foreign Assets Control (“OFAC”) have become an increasingly prominent part of U.S. foreign policy under the Trump administration. For the third year in a row, OFAC blacklisted more entities than it had under any previous administration, adding an average of 1,000 names to the Specially Designated Nationals and Blocked Persons (“SDN”) List each year—more than twice the annual average increase seen under either President Barack Obama or President George W. Bush. Targets included major state-owned oil companies such as Petróleos de Venezuela, S.A. (“PdVSA”), ostensible U.S. allies such as Turkey (and—almost—Iraq), major shipping lines, foreign officials implicated in allegations of corruption and abuse, drug traffickers, sanctions evaders, and more. As if one blacklisting was not enough, some entities had the misfortune of being designated multiple times under different regulatory authorities—each new announcement resulting in widespread media coverage if little practical impact. At last count, Iran’s Islamic Revolutionary Guard Corps (“IRGC”) has been sanctioned under seven separate sanctions authorities. Eager to exert its own authorities in what has traditionally been a solely presidential prerogative, in 2019 the U.S. Congress proposed dozens of bills to increase the use of sanctions. Compounding the impact of expansive new sanctions, OFAC’s enforcement penalties hit a record of more than U.S. $1.2 billion.

While President Obama described his sanctions team as his favorite “combatant command” (likening it to the traditional military forces employed by the United States), President Trump has truly unleashed the power of OFAC sanctions—employing them frequently, quickly, and unilaterally. The Trump administration announced new sanctions 82 times in 2019—eclipsing the previous record set in 2018. Much to the chagrin of the regulated community, more than one-quarter of the announcements in 2019 were made on a Friday. Under prior administrations, U.S. officials tried to avoid such late-week announcements to ensure that new designations were implemented consistently within the business week on both sides of the Atlantic. The willingness to impose Friday measures is an underappreciated indication of the breakdown in multilateral support for the use of U.S. sanctions, as well as the United States’ increasing willingness to go it alone.

This lack of multilateral sanctions engagement, however, should not be read as an indication that other jurisdictions are cooling to the idea of sanctions—quite the opposite. The United Kingdom, as a part of its Brexit process, announced that it would adopt existing European Union sanctions into its own domestic law in addition to promulgating independent, domestic measures that, at least initially, will target human rights abusers. The remainder of the European Union continued to threaten new measures against the regime of Venezuela’s Nicolás Maduro, paved the way for new sanctions against Iran by initiating the dispute resolution process allowed for under the Joint Comprehensive Plan of Action (“JCPOA”), and is considering sanctions targeting gross human rights violations. Meanwhile, companies began turning to the EU Blocking Statute—which aims to prohibit EU actors from complying with certain extraterritorial aspects of U.S. sanctions—to strengthen their position in contractual negotiations, disputes, and litigation.

Both China and Russia also proposed counter-sanctions in 2019 against parties who comply with U.S. measures. While China’s “unreliable suppliers” list has yet to be formalized and its sole counter-sanctions have thus far focused on non-economic actors

Related People

Judith Alison Lee

Adam M. Smith

Patrick Doris

Christopher T. Timura

Samantha Sewall

Audi K. Syarief

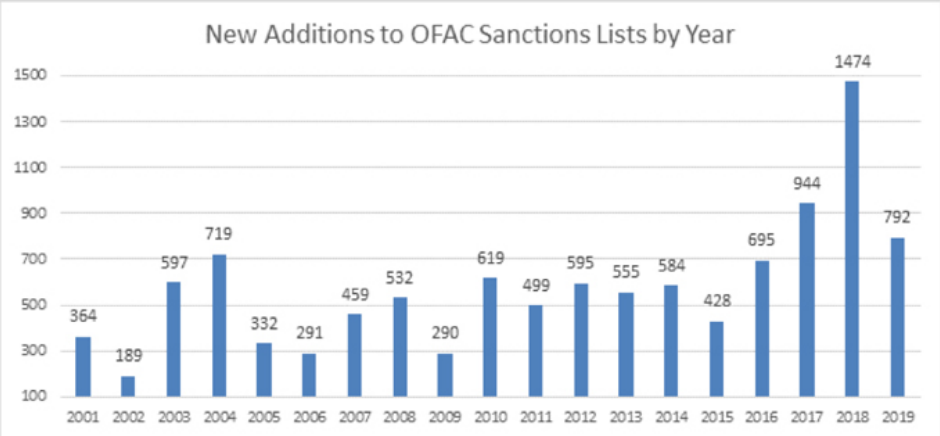
Scott R. Toussaint

(principally non-government organizations supportive of the Hong Kong democracy movement), and as of this writing Russian counter-sanctions remain un-enacted by the Duma, we expect the use of such counter-sanctions to increase in 2020.

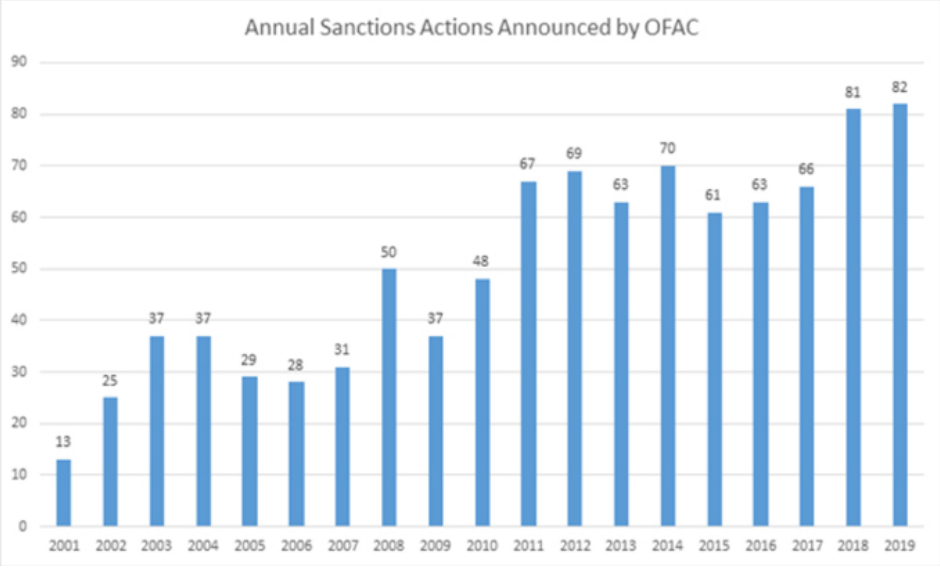
Though it is hard to predict how sanctions will develop going forward, we feel it is safe to assume that sanctions will remain a centerpiece of the current U.S. administration's approach to the world in 2020. We expect other world powers—both established and emerging—to respond in kind.

As the following charts illustrate, the two-decades-long trend toward increasing use of U.S. sanctions continued apace in 2019 and shows no signs of stopping during the year ahead.

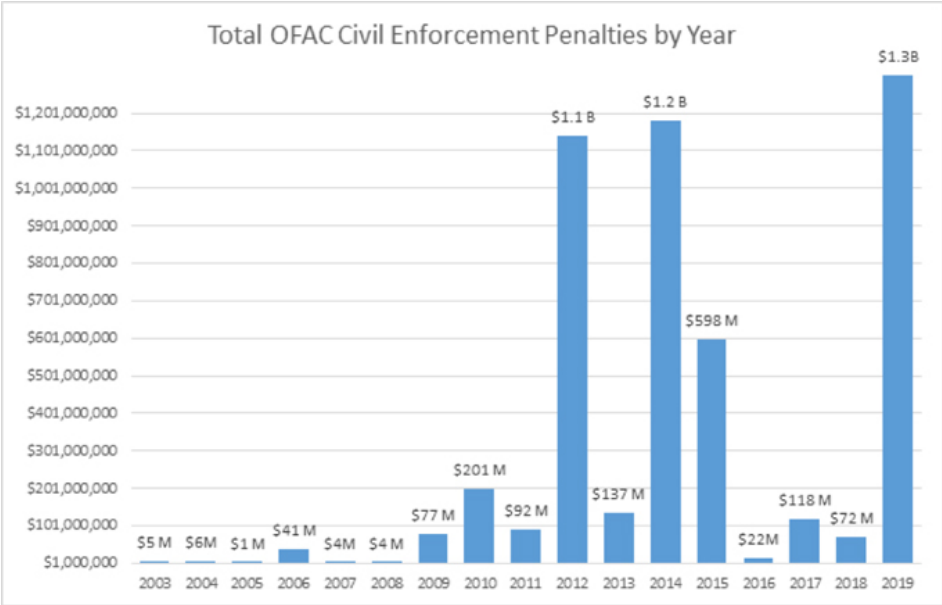
OFAC Designations



OFAC Sanctions Actions



OFAC Monetary Penalties



I. Major U.S. Program Developments

A. Iran

When the United States abandoned the JCPOA and fully re-imposed nuclear sanctions on Iran in November 2018, the Trump administration warned that the United States would exert "maximum economic pressure" on all facets of the Iranian economy to both deter Iran's "malign activities"—including its support for terrorism, missile proliferation, and regional disruption—and drive Iran back to the negotiating table. True to its word, the Trump administration continued to increase sanctions pressure on Iran and its trading partners in 2019 and expanded its enforcement efforts to new industries and institutions. Iran responded by pulling back from its commitments under the JCPOA, seeking alternative paths to avoid U.S. jurisdiction, and ramping up its provocative use of force. Hostilities with Iran escalated sharply by the end of the year—U.S. and Iranian-backed militias exchanged airstrikes and rocket attacks in late December, culminating in a militia-led breach of the U.S. embassy compound in Baghdad on December 31. When a U.S. airstrike killed Iranian General Qassem Soleimani on January 3, 2020, Iran vowed to retaliate, later carrying out a missile strike on two Iraqi military bases hosting U.S. troops. President Trump responded to this latest Iranian missile strike by promising the imposition of "additional punishing economic sanctions on the Iranian regime," a promise that left many observers questioning whether anything in Iran was left to be sanctioned.

In pursuing "maximum economic pressure," the United States has not only targeted new industries and entities but also has ramped up pressure on previously sanctioned persons. On April 8, 2019, as we described here, the United States designated the already-sanctioned IRGC as a foreign terrorist organization ("FTO"). Until this designation, the FTO label had been exclusively used on non-state actors, such as Al-Qaeda or the Islamic State of Iraq and Syria ("ISIS"). The FTO designation has limited practical impact, as the IRGC was already designated under several OFAC sanctions programs—including those related to counterterrorism.

As we discussed here, Iranian President Hassan Rouhani announced on May 8, 2019 that Iran would stop complying with the JCPOA's limitations on Iran's domestic build-up of enriched uranium and heavy water, and that same day President Trump signed an executive order authorizing new sanctions relating to the iron, steel, aluminum, and copper

sectors of the Iranian economy.

Notably, Iran has responded to increasing economic pressure—particularly on Iranian banks—by seeking alternative tools to finance its operations. Specifically, U.S. sanctions effectively cut off Iran's access to dollars and euros and contributed to a sharp drop in the value of the Iranian rial, making Iran's foreign reserve currencies an increasingly important tool for the support of Iran's activities in Iraq, Lebanon, Syria, and Yemen. According to OFAC, Iran used a network of Turkish and Emirati foreign exchange houses and front companies to exchange rials for foreign currencies used by a designated Iranian bank to support the IRGC's Qods Force ("IRGC-QF") and Iran's Ministry of Defense and Armed Forces Logistics ("MODAFL")—both of which have been designated to the SDN List. The United States responded to this workaround by designating 25 Iranian, Turkish, and Emirati exchange houses, trading companies, and officials on May 26, 2019. Rather than relying on its Iran sanctions authorities, OFAC used its counterterrorism sanctions—as it would later against Iran's central bank—to ensure maximum impact. Entities designated under that program are not only subject to the broad sanctions restrictions typically imposed on SDNs but also may not participate in humanitarian trade with Iran—a category of activity generally exempt from sanctions restrictions. The designations also underscored OFAC's willingness to extend its maximum economic pressure campaign to Iran's international supporters, a possible harbinger of things to come in 2020.

In 2019, the United States continued to roll back sanctions relief that it had previously provided to other countries, including waivers that allowed certain jurisdictions to continue importing Iranian oil. In particular, waivers granted to China, India, South Korea, Japan, Italy, Greece, Taiwan, and Turkey allowed those jurisdictions to continue importing Iranian oil without being sanctioned by the United States, provided that those jurisdictions significantly reduced their Iranian oil imports. Our analyses of these temporary waivers, also known as Significant Reduction Exceptions ("SREs"), can be found here and here. The Trump administration also announced that, as part of its maximum pressure campaign, no further SREs would be issued and warned that those who continued to trade in Iranian crude would be sanctioned. The expiration of the SREs had relatively little effect on Taiwan, Italy, and Greece, which reportedly ceased importing oil from Iran long before the announcement.

By contrast, China *increased* its purchases of Iranian oil, cementing its status as Iran's biggest customer. According to the U.S. State Department, China continued to purchase oil from Iran following the expiration of its SRE in May. In response, the Trump administration made good on its earlier warning—quickly sanctioning a Chinese state-owned oil trading company and its CEO in July. In announcing the designation, Secretary of State Mike Pompeo emphasized that the United States takes its secondary sanctions seriously and "will sanction any sanctionable behavior." That warning, combined with the speed of the designation and the targeting of a state-owned firm, sent a clear signal that the Trump administration would continue aggressively applying maximum economic pressure both within and outside Iran.

In one of the more disruptive sanctions actions of the past year, OFAC on September 25, 2019, designated two subsidiaries of the giant Chinese company COSCO Shipping Corporation Ltd. ("COSCO") for their involvement in transporting Iranian oil. While this action targeted only approximately 40 vessels belonging to the two designated entities (and their majority-owned subsidiaries), by not identifying those vessels by name the designation caused confusion to ripple through world markets regarding which among the approximately 1,100 vessels in the larger COSCO fleet were actually subject to U.S. sanctions. In an abundance of caution, many counterparties temporarily ceased doing business with all COSCO vessels—leaving numerous ships and their cargo stranded at sea. This confusion dissipated only after OFAC issued guidance indicating that non-U.S. persons that continue to deal with COSCO post-designation will generally not be at risk of U.S. sanctions exposure provided that such dealings do not involve Iran or otherwise have any U.S. nexus, and also issued a general license authorizing U.S. person involvement in transactions and activities ordinarily incident to the maintenance and wind down of pre-

existing contracts involving one of the two sanctioned COSCO entities and its vessels.

In another example of the Trump administration's maximum pressure campaign reaching beyond the typical industries, OFAC released an advisory on July 23, 2019 warning of Iran's deceptive practices in the civil aviation industry and the heightened risk of enforcement actions against those that engage with Iran. The advisory formally put the global commercial aviation industry on notice of the role Iranian commercial airlines play in providing services to the Iranian government and military, as well as the deceptive practices commonly used to acquire U.S.-origin aircraft and related goods—including using front companies, misrepresenting that sanctions have been lifted, and falsely claiming OFAC authorization. The guidance specifically called out Mahan Air—designated in 2011 for its support of the IRGC-QF—for flying several flights per week with fighters and weapons to Damascus, and flying back the bodies of Iranian soldiers killed in Syria. The industry advisory used more than just the threat of sanctions to urge the civil aviation industry to avoid Mahan, noting that Germany and several other countries deny Mahan landing rights and urging others to do the same, as well as warning that Mahan has failed to pay its debt obligations.

As sanctions began to bite, economic tensions escalated to physical conflict. In September, Iran conducted airstrikes on Saudi Arabian oil facilities. The United States responded by imposing additional sanctions on the Central Bank of Iran ("CBI") and Iran's sovereign wealth fund on September 20. The United States accused those entities of supporting the IRGC, its Qods Force, and Hezbollah, and designated them using OFAC's primary counterterrorism authority. Although President Trump characterized these designations as the "highest sanctions ever imposed on a country," these sanctions in fact marked the latest in a series of actions targeting the CBI, including its earlier designation to the SDN List in November 2018. OFAC had also previously sanctioned senior CBI officials for their involvement in transactions supporting the IRGC and its Qods Force. These earlier sanctions already prohibited U.S. persons from engaging in transactions involving CBI and its designated officers, and non-U.S. persons were already subjected to secondary sanctions for doing so.

The new counterterrorism designations primarily impact the ability of U.S. and non-U.S. persons to provide food, other agricultural products, medicine, and medical devices to Iran. Such humanitarian goods can typically be provided to Iran pursuant to a general license. However, the license expressly prohibits the involvement of persons designated under OFAC's counterterrorism sanctions—now including the CBI. Given the CBI's key role in financing and otherwise facilitating humanitarian trade with Iran, many were concerned that the provision of humanitarian items to Iran had effectively become unlawful or sanctionable.

In response to these concerns, OFAC announced that it would implement a new mechanism to identify compliant financial channels to support humanitarian exports to Iran. According to Brian Hook, the U.S. Special Representative for Iran, the new financing channel would "make it easier for foreign governments, financial institutions, and private companies to engage in legitimate humanitarian trade on behalf of the Iranian people while reducing the risk that money ends up in the wrong hands."

Under the new program, OFAC will provide written confirmation, or "comfort letters," that proposed financial channels are not exposed to U.S. sanctions. However, to obtain these comfort letters, exporters of humanitarian items, foreign financial institutions, and foreign governments will be required to provide, on an ongoing basis, a significant amount of detailed information about their Iran-related activities and the proposed payment channel. Specifically, OFAC will require those seeking written confirmation to submit monthly reports that include detailed information about Iranian customers, their beneficial ownership, the seller of the items for export, the items included in the proposed exports, and the path of the export. Those who obtain written confirmation from OFAC will also be required to inform OFAC if they discover that their Iranian customers have misused the financial channel for non-humanitarian purposes. As of this writing, we are aware of no

companies that have yet taken OFAC up on its offer.

On December 11, 2019, OFAC followed its warning to the civil aviation industry with the designation of three of Mahan's general sales agents, which are third parties that provide services to an airline under the airline's brand. None of the sales agents are based in Iran; the designated entities are registered in the United Arab Emirates and China. They were all designated purely for acting on behalf of Mahan Air, and were not alleged to have specifically been involved in flights to and from Syria.

On January 10, 2020, OFAC announced the designation of several senior Iranian government officials, as well as Iran's largest steel, aluminum, copper, and iron manufacturers, a number of Iranian metal producers, and several Chinese and Seychellois companies involved in the purchase of Iranian metals. The President also issued a new executive order authorizing OFAC to designate entities operating in Iran's construction, mining, manufacturing, or textile sectors *or any other sector* of the Iranian economy determined by the U.S. Secretary of the Treasury and authorizing the imposition of secondary sanctions for any entity that supports Iranian companies designated under the new authority. Following the U.S. drone strike that killed General Soleimani, Iran again announced that it would further reduce its commitments to restrain its nuclear program and would no longer comply with the restrictions on the number of centrifuges it may operate. The most meaningful response to Iran's actions may come from the European Union which has triggered the dispute mechanism under the JCPOA—which could lead to the automatic re-imposition of sanctions against Iran.

With much of Iran now subject to comprehensive, sometimes overlapping sanctions regimes, it is not clear whether and how the Trump administration will continue to increase sanctions pressure on Iran. OFAC may target additional Iranian government officials, and 2020 will likely see designations under the newly released executive order targeting Iran's construction, mining, manufacturing, and textiles sectors. If past is prologue, the Trump administration may also begin imposing secondary sanctions more robustly in an effort to further cut off Iran's international support. These measures may have limited practical impact, however, as many non-U.S. entities have already decided not to participate in the Iranian economy out of concern for the tightening network of U.S. secondary sanctions.

B. Venezuela

U.S. sanctions targeting the regime of Venezuela's President Nicolás Maduro significantly expanded in 2019, as the Trump administration designated the giant state-owned oil company PdVSA, the country's central bank, and ultimately the entire Government of Venezuela. These seismic shifts in U.S. policy were prompted by a power struggle in Caracas between Nicolás Maduro and Juan Guaidó, the head of Venezuela's National Assembly, that witnessed dueling claims to the presidency, widespread public protests, and an abortive military uprising. Against that tumultuous backdrop, the United States sought to hasten the transition to a democratically elected government by imposing more than 20 rounds of sanctions designed to deny the Maduro regime the financial resources to sustain its hold on power. In addition to designating progressively broader segments of the Venezuelan state, the Trump administration during 2019 also expanded U.S. sanctions to target Venezuela's oil, financial, and defense and security sectors; a growing list of senior regime officials; as well as President Maduro's perceived enablers in Russia and Cuba.

The rapid evolution of U.S. sanctions on Venezuela began immediately after the new year. In January 2019, Nicolás Maduro was inaugurated for a second term as president following an election widely described by outside observers as neither free nor fair. Within days, Juan Guaidó, acting as head of the National Assembly—the country's sole remaining democratic institution—invoked a provision of Venezuela's constitution to declare himself the country's interim leader. (Guaidó's claim to be Venezuela's lawful head of state has since been recognized by the United States and nearly 60 other countries.) In a protective

action designed to deny Maduro and his inner circle access to oil revenues and to prevent the regime from looting state assets, the Trump administration on January 28, 2019, imposed sanctions on the state-owned oil company PdVSA—by far the most economically significant actor in Venezuela's oil-driven economy and one of the largest companies ever designated by OFAC. PdVSA's designation and its implications are described at length in an earlier client alert, available here. Underscoring the strong U.S. policy interest in preserving PdVSA for use in rebuilding Venezuela's economy under a post-Maduro government, OFAC has issued and repeatedly extended general licenses authorizing certain transactions involving PdVSA's main U.S. subsidiary CITGO, as well as the activities of five named U.S. oil and oil services companies that operate joint ventures with PdVSA.

As the year progressed, the Trump administration continued to make use of the authorities set forth in Executive Order 13850—which empowers the U.S. Secretary of the Treasury to impose sanctions on persons who operate in the gold sector of the Venezuelan economy, and any other sector the Secretary deems appropriate—to target areas of the Venezuelan economy that generate large amounts of hard currency and are especially prone to corruption. In particular, OFAC during 2019 used this authority to impose sanctions on specific individuals and entities operating in the gold, oil, financial, and defense and security sectors of Venezuela's economy. Among the targeted entities were the state gold mining company, Minerven; PdVSA's majority-owned subsidiaries; Venezuela's national development bank, BANDES, and four of its affiliates, including the prominent commercial lender Banco de Venezuela; and the Central Bank of Venezuela. Taken together, these measures sharply constrained the Maduro regime's access to capital and closed off key channels for transferring funds in and out of Venezuela.

In August 2019, the United States went further and imposed sanctions on the entirety of the Government of Venezuela, including all of its agencies and political subdivisions. Importantly, however, this measure did not impose sanctions on all transactions involving the *country* of Venezuela and its practical impact was limited by the fact that the most economically significant arms of the Venezuelan state—including the national oil company, PdVSA, and its various subsidiaries, along with the country's central bank—were already subject to U.S. sanctions. OFAC then further cabined this action by issuing general licenses—common across even the most restrictive U.S. sanctions programs (such as those targeting Cuba, Iran, North Korea, and the Crimea region)—authorizing certain transactions that involve the Venezuelan government and that are associated with telecommunications/mail; technology allowing internet communication; medical services; registration and defense of intellectual property; support for non-governmental organizations; transactions related to port and airport operations; overflight payments; and personal maintenance of U.S. persons inside Venezuela. Further details regarding this action can be found in our August 2019 client alert.

Throughout the past year, the United States also sought to target the Maduro regime's perceived enablers, both within Venezuela and abroad. Consistent with past practice, the United States continued to designate a steady stream of senior Venezuelan government officials, including the country's foreign minister and various members of the security services. Such designations appear designed both to punish previous bad behavior by senior officials—including corruption, mismanagement and the breakdown of democratic institutions—and to deter other officials from engaging in similar conduct in the future. Additionally, the Trump administration designated numerous foreign actors—principally from Russia and Cuba—for providing a financial lifeline to the government in Caracas. For example, in March 2019, OFAC designated the Russian-Venezuelan financial institution Evrofinance Mosnarbank for helping the regime to evade U.S. sanctions by, among other things, financing Venezuela's cyber currency, the Petro. OFAC, across multiple actions, also designated dozens of companies and vessels involved in the Venezuela-Cuba oil trade, and has strongly suggested that Russian and Chinese individuals and entities may be sanctioned if they continue to prop up the Maduro regime.

Finally, amid a year of sweeping changes to the Venezuela sanctions program, OFAC has

repeatedly emphasized that “U.S. sanctions need not be permanent and are intended to bring about a positive change of behavior.” Even if such an “off ramp” to sanctions has always existed—and parties do come off the SDN List—OFAC’s announcement that it would be amenable to de-listing parties if they manifest a change in behavior is new. Along those lines, the Trump administration has held out the prospect of sanctions relief for individuals and entities that renounce their previous support for President Maduro—an enticement OFAC has touted by de-listing the former head of Venezuela’s intelligence service, along with numerous shipping companies and vessels that had discontinued their Venezuela-related business activities and implemented sanctions compliance measures. Moreover, OFAC has indicated in published guidance that it is prepared to swiftly lift sanctions on PdVSA, and presumably the Government of Venezuela itself, upon a transfer of control “to Interim President Juan Guaidó or a subsequent, democratically elected government.” Accordingly, just as the United States rapidly tightened sanctions on Venezuela during 2019, there remains the possibility, if President Maduro were to fall, that U.S. sanctions could be eased just as quickly.

C. Cuba

In 2019, the Trump administration continued to reverse the Obama administration’s easing of measures on Cuba. In April 2019, President Trump removed a more than two-decades-long restriction on American citizens’ ability to bring suit over property confiscated by the Cuban regime. Title III of the Cuban Liberty and Democratic Solidarity (LIBERTAD) Act of 1996, commonly known as the Helms-Burton Act, authorizes U.S. citizens and companies whose property was confiscated by the Cuban government to sue those that “traffic” in that confiscated property. Since the Act’s entry into force in 1996, Presidents of both parties had continuously suspended the availability of this cause of action. As we discussed here, by lifting this suspension President Trump has—for the first time—opened up U.S. federal courts to a new type of lawsuit, which has important implications not only for U.S. relations with Cuba but also with countries that continue to operate in Cuba.

Title III actions can be based on claims certified by the Foreign Claims Settlement Commission of the United States (“FCSC”)—a quasi-judicial, independent federal agency created by the International Claims Settlement Act of 1949 (“certified claims”), or claims that have not been adjudicated by the FCSC process (“uncertified claims”). There are currently 6,000 certified claims, and by the State Department’s estimate, up to 200,000 uncertified claims. We have not yet witnessed a flood of litigation; rather, the filing of new Title III cases has averaged a little over two cases per month. By Gibson Dunn’s count, there have been 21 Title III cases filed in federal court to date, with the vast majority in the Southern District of Florida. Many of these cases were brought against defendants in the tourism industry, including airlines, cruise lines, hotels, and travel technology companies, with a number related to other industries such as oil refining, banking, and farming.

Also in April 2019, the Trump administration struck down a December 2018 deal between ***Major League Baseball*** (“MLB”) and the ***Cuban Baseball Federation*** (“CBF”) in which Cuban athletes would have been allowed to play in the United States without defecting. Under the MLB-CBF deal, an MLB team could sign a CBF player if it, among other things, paid the CBF a fee equivalent to 25% of the player’s signing bonus. (A similar arrangement exists for foreign players from other countries such as Japan.) The deal was originally thought to be authorized under a license established by the Obama administration that allowed the hiring of a Cuban national as long as payments were not made to the Cuban government in connection with such hiring. Per a senior Trump official, although this license remains in effect, the CBF is considered a part of the Cuban government and, as a result, the MLB-CBF deal as structured was illegal.

In June 2019, OFAC announced it would no longer authorize “people-to-people” educational group travel, which had allowed an organization subject to U.S. jurisdiction to sponsor exchanges that promoted contact with Cuban locals. Those travelers who had

completed at least one travel-related transaction (e.g., purchasing a flight, booking a hotel) prior to June 5, 2019 were grandfathered in and allowed to proceed with their trip. Notably, OFAC left intact the "support for the Cuban people" travel authorization which also allows travel to Cuba but under strict conditions, such as avoiding all state-run businesses and institutions.

At the same time, the U.S. Commerce Department's Bureau of Industry and Security ("BIS"), in coordination with OFAC, instituted a policy of denying licenses for passenger and recreational vessels (e.g., cruise ships, yachts), and private and corporate aircraft, to travel to Cuba on temporary sojourn. Moreover, such vessels and aircraft were made ineligible for license exceptions. This policy change left cruise lines scrambling to modify their trips.

In September 2019, OFAC announced a number of changes to the general license allowing for remittances to Cuba. First, the amount that one remitter can send to one Cuban national was capped at $1,000 per quarter. Second, close relatives of Cuban government officials or Cuban Communist Party officials could no longer be the recipients of such remittances. (The officials themselves had already been barred.) Third, "donative" remittances to certain individuals and organizations under 31 C.F.R. § 515.570(b) were eliminated. In that same action, OFAC also created a new authorization that allows for remittances to "self-employed individuals," which includes small business owners, contractors, and farmers.

At the same time, OFAC announced changes to the "U-Turn" general license. The U-Turn license authorized U.S. financial institutions to "process fund transfers originating and terminating outside the United States, provided that neither the originator nor the beneficiary is a person subject to U.S. jurisdiction." In effect, this allowed transactions between a Cuban national and a non-U.S. person, occurring outside the United States, to be conducted using U.S. dollars processed through the U.S. financial system via correspondent accounts maintained at U.S. intermediary banks. Now, such institutions are required to reject requests for these transactions. While this change dramatically limits the ability of Cubans to transact in U.S. dollars, notably banks are not required to block the funds at issue.

The Trump administration gave the same rationale for these financial restrictions as they did for the travel restrictions months earlier. As Treasury Secretary Steven Mnuchin expressed it, by imposing these restrictions, the United States is "hold[ing] the Cuban regime accountable for its oppression of the Cuban people and support of other dictatorships throughout the region, such as the illegitimate Maduro regime."

In October 2019, citing Cuba's "destructive behavior at home and abroad," BIS amended the Export Administration Regulations ("EAR") in a number of ways to further restrict exports and re-exports of items to Cuba. First, licenses to lease aircraft to Cuban state-owned airlines were revoked, and a general policy of denying future applications was instituted. Second, the *de minimis* level was revised downward for Cuba from 25% to 10%, meaning that items with at least 10% Cuban content would be subject to EAR restrictions. Third, the "Support for the Cuban People" license exception was limited in a number of ways, including barring donations to organizations controlled by or administered by the Cuban government or the Cuban Communist Party.

In addition to changes to the Cuba sanctions regulations, the Trump administration has consistently added Cuban persons and entities to the blacklist for their support of Venezuela's Maduro regime. As discussed above, numerous shipping entities and vessels that have transported Venezuelan oil to Cuba have been sanctioned along with Cuban state-owned oil companies and individual Cuban government officials. Cuba's defense minister, for example, has been barred by the U.S. State Department from entry into the United States for his actions "prop[ping] up the former Maduro regime in Venezuela."

D. North Korea

Amid the stalled nuclear negotiations between President Trump and North Korean leader Kim Jong Un, the United States over the past year continued to target the illicit movement of goods in and out of North Korea. On March 21, 2019, OFAC published an advisory to address North Korea's illicit shipping practices (the "North Korea Advisory"). That document serves as a comprehensive guide to key participants in the shipping trade, such as ship owners, financial institutions, brokers, oil companies, port operators, and insurance companies, and includes an overview of sanctions specific to the shipping industry. The North Korea Advisory also includes updated information about North Korea's deceptive shipping practices, as well as additional guidance for members of the shipping industry on how to mitigate the risk of involvement in these practices.

According to OFAC, North Korea has been resorting to certain tactics to mask the identities of vessels and cargo in order to evade U.S. sanctions. These tactics include: (i) disabling a vessel's location-tracking Automatic Identification System ("AIS"); (ii) physically altering a vessel's identification or International Maritime Organization number; (iii) engaging in ship-to-ship transfers to conceal the origin or destination of the transferred cargo; (iv) falsifying cargo and vessel documents; and (v) manipulating data transmitted via AIS. To counter these deceptive practices, the North Korea Advisory encourages persons involved in shipping-related transactions to adopt certain risk mitigation measures, including but not limited to, carrying out necessary diligence to verify the identity of vessels, reviewing all applicable shipping documentation, and monitoring for AIS manipulation and disablement. The North Korea Advisory also identifies, in a series of annexes, 18 vessels believed to have engaged in ship-to-ship transfers with North Korean tankers, plus 49 vessels that are believed to have exported North Korean coal since the United Nations Security Council Resolution 2371 was passed on August 5, 2017.

Throughout 2019, OFAC continued to designate individuals and entities involved in the shipping industry for facilitating North Korean trade. On March 21, 2019, OFAC designated two Chinese shipping companies for their dealings with North Korea, citing the routine use of deceptive practices that enabled EU-based North Korean procurement officials to operate and purchase goods for the Kim regime. On August 30, 2019, OFAC announced North Korea-related designations of two individuals and three entities from Taiwan and Hong Kong for participating in illicit "ship-to-ship transfers" to enable North Korea's import of refined petroleum products. Finally, U.S. prosecutors continued to pursue civil forfeiture actions against companies engaged in the illicit shipment of goods to North Korea, relying in many instances on money laundering or bank fraud charges in addition to violations of OFAC sanctions.

E. Russia

In 2019, OFAC took additional measures to address and combat Russia's past and current attempts at interfering in the U.S. electoral process. On September 30, 2019, OFAC took its first action under Executive Order 13848, targeting Russia's Internet Research Agency ("IRA") and its financier, Yevgeniy Prigozhin, as well as entities, individuals, and assets associated with them, for their efforts to interfere with the 2018 midterm elections. Executive Order 13848, which was announced in September 2018, blocks all property in the United States of those who have "directly or indirectly engaged in, sponsored, concealed, or otherwise been complicit in foreign interference in a United States election," as well as those found to have provided support for election interference. The action's practical impact was limited by the fact that both the IRA and Prigozhin were previously designated in March 2018 under Executive Order 13694, which the Obama administration implemented to target "malicious cyber actors," as were four of the six IRA members who were designated in this action. Adding additional pressure to Prigozhin, OFAC designated three of his private aircraft, a yacht, and three entities that operated those vessels.

On August 3, 2019, the Trump administration announced that OFAC will be issuing a second round of sanctions in response to Russia's use of the Novichok nerve agent in the United Kingdom in March 2018. The Chemical and Biological Weapons Control and Warfare Elimination Act of 1991 (the "CBW Act") requires, in the event that the President determines that a foreign government has used chemical or biological weapons, two rounds of sanctions. This second round of CBW Act sanctions prohibits U.S. banks, including foreign branches, from participating in the primary market for non-ruble denominated bonds issued by Russia and from issuing non-ruble denominated loans to Russia. As detailed in our 2018 Year-End Sanctions Update, the first round of sanctions were imposed on August 22, 2018. Though initially expected in November 2018, the second round of sanctions was not implemented until August 26, 2019, over a year after the first round's implementation.

As described in detail here, on April 6, 2018, OFAC significantly enhanced the impact of sanctions against Russia by blacklisting almost 40 Russian oligarchs, officials, and their affiliated companies pursuant to Obama-era sanctions, as modified by the Countering America's Adversaries Through Sanctions Act of 2017. On December 19, 2018, OFAC de-listed three entities that had been related to sanctioned oligarch Oleg Deripaska after the companies took significant steps to disentangle from Deripaska's ownership.

Several months later, on March 15, 2019, Deripaska sued the Secretary of the Treasury, the Department of the Treasury, and OFAC in U.S. federal court in order to reverse the sanctions imposed upon him. Deripaska argued that OFAC acted outside the bounds of its authority by including him on "an arbitrarily contrived list of 'oligarchs'" and that "[t]he effects of these unlawful sanctions has been the wholesale devastation of [his] wealth, reputation, and economic livelihood." Although the U.S. government has filed a motion to dismiss (and, in the alternative, motion for summary judgment) and Deripaska has submitted his opposition, the court has stayed the motion until the parties file a joint status report, due on February 19, 2020.

Congress and the Trump administration took additional measures against Russia during the very last weeks of 2019, highlighting the geopolitical tension between the two countries.

On December 18, 2019, the Senate Foreign Relations Committee voted to approve the Defending American Security from Kremlin Aggression Act ("DASKA"), which aims to impose new sanctions on the Russian financial, energy, and cyber sectors. The draft bill limits the President's ability to withdraw from NATO, establishes in the State Department a new office to address international cybersecurity, creates new offenses related to hacking, and directs the President to impose a host of sanctions against Russia. Among the many contemplated sanctions, the bill includes additional sanctions against Russian banks, the Russian energy, cyber, and shipbuilding sectors, sovereign debt, and, significantly, sanctions on persons who facilitate corrupt activities on behalf of President Vladimir Putin. Although the bipartisan bill has been dubbed the bill "from hell," currently there is no scheduled date for the full Senate to vote on its adoption.

Two days after DASKA was approved by committee, the President signed the National Defense Authorization Act for Fiscal Year 2020 (the "NDAA"), which includes provisions requiring the imposition of sanctions against vessels and persons involved in the construction of two Russian gas export pipelines, the Nord Stream 2 and the Turkstream pipelines. Although the inclusion of these sanctions signals U.S. support for Ukraine—Russia is constructing these pipelines largely to bypass Ukraine—their impact may be minimal as the pipelines' construction is nearly complete.

F. Syria

As we described in an earlier client alert, on October 14, 2019, the Trump administration authorized sanctions against core ministries of the Government of Turkey in response to

Ankara's incursion into northern Syria. Shortly thereafter, OFAC issued sanctions against Turkey's Ministry of Energy and Natural Resources and Ministry of National Defense, as well as three senior officials. Less than two weeks later, following the announcement of a ceasefire in northern Syria, the Department of Treasury delisted the two ministries and three senior officials. To our knowledge, OFAC had never issued and then reversed sanctions so quickly against such significant targets.

On March 25, 2019, OFAC issued an updated advisory to the maritime petroleum shipping community "alert[ing] persons globally to the significant U.S. sanctions risks for parties involved in petroleum shipments to the Government of Syria" (the "Syria Advisory"). That document emphasizes that certain countries, in particular Iran and Russia, ship petroleum to Syria, and that the facilitation of such transactions by persons subject to U.S. jurisdiction puts those persons at risk for being targeted by OFAC. The Syria Advisory also includes a non-comprehensive list of deceptive practices employed by certain shipping companies to "obfuscat[e] the destination and recipient of oil shipments in the Mediterranean Sea ultimately destined for Syria," as well as certain measures companies should take to mitigate risk presented by these practices.

Though very similar to an earlier advisory on which it is based, the latest version of the Syria Advisory includes "additional guidelines and risks associated with facilitating the shipment of petroleum destined for Syrian Government-owned and -operated ports, to include petroleum of Iranian origin." Additionally, the updated Syria Advisory includes an expanded annex, listing additional vessels that are alleged to have delivered petroleum to Syria between 2016 and 2018, as well as vessels that are alleged to have engaged in ship-to-ship transfers of oil destined for Syria and those that had exported Syrian oil to other countries.

II. Other OFAC Programs

A. Global Magnitsky Sanctions

As we noted previously, on December 20, 2017, President Trump issued Executive Order 13818, an unusually broad executive order to implement the Global Magnitsky Human Rights Accountability Act ("Global Magnitsky Act"), a 2016 law that authorizes sanctions against those responsible for human rights abuses and significant government corruption around the world.

The Global Magnitsky Act is named for Sergei Magnitsky, a Russian accountant who was imprisoned after exposing a tax fraud scheme allegedly involving Russian government officials and who died under suspicious circumstances while in custody. The 2012 Sergei Magnitsky Rule of Law Accountability Act of 2012 (the "2012 Magnitsky Act") authorizes sanctions against individuals and entities found to have been involved in Magnitsky's mistreatment and death as well as subsequent efforts to obstruct the related investigation. The Global Magnitsky Act expands that sanctions authorization to cover serious human rights abuses and corruption worldwide.

In 2019, the Trump administration designated 97 individuals and entities under the Global Magnitsky Act. That figure was nearly double the 49 designations in 2018, a significant number of which were levied against those involved in the killing of the journalist Jamal Khashoggi. Together with the initial round of designations that accompanied issuance of Executive Order 13818, the total number of persons designated pursuant to the Global Magnitsky Act is currently 196 (two designations of senior Turkish government officials were lifted in 2018 following the release of American pastor Andrew Brunson). Also this past year, the administration designated six additional Russian persons pursuant to the 2012 Magnitsky Act.

On December 9 and 10, 2019, in conjunction with International Anticorruption Day and International Human Rights Day, respectively, OFAC announced a set of wide-ranging

sanctions targeting notable cases of public corruption and serious abuses.

On December 9, 2019, Treasury announced the following Global Magnitsky Act designations:

- Try Pheap and Kun Kim, current and former senior Cambodian officials responsible for significant public corruption and misuse of state resources.
- Aivars Lembergs, a Latvian oligarch and mayor of Ventspils, Latvia, who is involved in significant public corruption, money laundering, and abuse of office. OFAC also designated four entities controlled by Lembergs, including the Ventspils Freeport Authority.
- Associates of and entities controlled by Slobodan Tesic, a Serbian arms dealer who was previously sanctioned by the UN for violating the arms embargo imposed on Liberia.

On December 10, 2019, Treasury announced the following designations:

- Four senior Burmese military officials, including the Commander-in-Chief of the Burmese military forces, for their involvement in serious human rights abuses committed against the minority Rohingya people in Rakhine State. Since 2017, over 500,000 Rohingya have fled Burma and, during that time, the Burmese military has been engaged in acts of mass violence directed against the Rohingya people.
- The leader and deputies of the Allied Democratic Forces (“ADF”) of the Democratic Republic of the Congo (“DRC”). The ADF has engaged in serious human rights abuses, committing acts of mass violence, torture, abduction, and the use of child soldiers for over two decades in the Eastern part of the DRC, near the border with Uganda.
- Marian Kocner, a Slovakian businessman, charged with ordering the murder of Jan Kuciak, a young reporter who had uncovered alleged corrupt dealings involving Kocner.
- A Pakistani senior superintendent of police reportedly responsible for staging encounters in which over 400 individuals were killed by police.

OFAC also used the Global Magnitsky authority to target several Iraqi officials, some of whom are known proxies of the IRGC-QF. In July 2019, Treasury designated two Iraqi militia leaders pursuant to the Global Magnitsky Act for human rights abuses and corruption carried out in the Nineveh region of Iraq, a former Islamic State stronghold, as well as two Iraqi former politicians accused of significant public corruption. In December 2019, Treasury designated three Iraqi militia leaders responsible for directing soldiers to open fire on protesters in Baghdad. The Iraqi militia leaders were described as proxies of the IRGC-QF. The designations were made just weeks before one of the designated militia leaders was photographed among those protesting at the U.S. Embassy in Baghdad on December 31. On January 3, 2020, two of the previously designated militia leaders were further designated as global terrorists.

As discussed further below, the European Union announced on December 9, 2019 that it would begin drafting its own Magnitsky-style sanctions framework for targeting human rights offenders. The United Kingdom and Canada have already adopted Magnitsky-style sanctions programs.

From a compliance perspective, the Global Magnitsky Act designations serve as a reminder to carefully assess contacts with, and screen business partners related to, jurisdictions of heightened concern, even if those jurisdictions are not subject to comprehensive sanctions. Particularly with respect to jurisdictions with increased risk related to public corruption, organized crime, or geopolitical instability, sanctions may be

deployed with very little notice and may affect commercial networks both within and beyond the country concerned.

B. Narcotics Trafficking Kingpin Sanctions and New Fentanyl Sanctions Act

This past year brought renewed focus on using financial sanctions to target persons involved in the international trafficking of opioids. On August 21, 2019, the Treasury Department announced coordinated action by OFAC and by Treasury's Financial Crimes Enforcement Network ("FinCEN") to target manufacturers and distributors of illicit synthetic opioids. OFAC designated three Chinese individuals and two entities pursuant to the Foreign Narcotics Kingpin Designation Act ("Kingpin Act") for operating an international drug trafficking network responsible for shipping hundreds of packages of synthetic opioids to the United States. Treasury highlighted the use of digital currency by the designated persons to launder the proceeds of illicit drug sales. The White House also announced actions to crack down on international fentanyl trafficking, including the publication of a series of private-sector advisories to help domestic and foreign businesses protect themselves and their supply chains from inadvertent fentanyl trafficking.

Congress took further action by adopting the Fentanyl Sanctions Act on December 20, 2019, as Title 72 of the NDAA. The Act requires the President to submit to Congress within 180 days a list of persons determined to be foreign opioid traffickers and requires the imposition of five or more sanctions measures against such persons, including, among other restrictions, an asset freeze, visa ban, exclusion from public procurement, and exclusion from the U.S. financial system. The statute also calls upon the government of China to follow through on its commitments to implement new regulations controlling the production and export of fentanyl and fentanyl analogues.

Separately, OFAC designated over 70 additional persons under the Kingpin Act in 2019, including drug trafficking and money laundering networks in Argentina, the Dominican Republic, Guatemala, Lebanon, Mexico, and the United Arab Emirates.

C. Mali

Despite the presence of 15,000 United Nations peacekeepers and police in Mali, renewed violence has continued to roil the country; news reports indicate that at least 200,000 people were displaced in the first half of 2019 alone. As a result, the Trump administration on July 26, 2019, announced a new sanctions program "to combat the worsening situation in Mali," which was described to include "[m]align activities such as drug trafficking, hostage taking, attacks against civilians, and attacks against United Nations (UN) Multidimensional Integrated Stabilization Mission in Mali (MINUSMA) personnel." In connection therewith, President Trump issued Executive Order 13882, finding the deterioration of peace and security in Mali to constitute a national security threat to the United States.

The Order blocks all property and interests in property under U.S. jurisdiction of persons determined to be responsible or complicit in: acts or policies that threaten the peace, security, stability, or the democratic processes or institutions in Mali; acts that threaten, violate, or obstruct the 2015 Agreement on Peace and Reconciliation in Mali; planning or sponsoring attacks against government institutions and the Malian defense and security forces, international security forces and peacekeepers, and any other U.N. personnel; obstructing the distribution of humanitarian aid; planning, directing, or committing any act that violates international humanitarian law or constitutes a serious human rights abuse; the use or recruitment of child soldiers in the Malian armed conflict; the illicit production of or trafficking in narcotics; trafficking in persons, arms, and illegally acquired cultural property; and any transaction(s) involving bribery or other corruption. Currently, five individuals have been added to the SDN List pursuant to this Order.

III. Other U.S. Developments

A. New Treasury Under Secretary for Terrorism and Financial Intelligence

On December 10, 2019, the Trump administration announced its intent to nominate Jessie K. Liu, the United States Attorney for the District of Columbia, to the position of Under Secretary for Terrorism and Financial Intelligence at the Treasury Department, a role previously held by Sigal Mandelker. In this role, Liu would lead the Treasury Department teams responsible for administration and enforcement of U.S. sanctions programs. Liu previously served as Deputy General Counsel of the Treasury Department and in a senior position within the Justice Department's National Security Division, the office responsible for criminal enforcement of U.S. sanctions and export control laws.

B. OFAC Compliance Guidance

As we described in a previous client alert, OFAC in May 2019 published "A Framework for OFAC Compliance Commitments," on what constitutes an effective sanctions compliance program. The document represents the most detailed statement to date of OFAC's views on the best practices that companies should follow to ensure compliance with U.S. sanctions laws and regulations. Importantly, this guidance also aims to provide greater transparency with respect to how, should a sanctions violation occur, OFAC will assess the adequacy of a company's existing compliance program in determining what penalty to impose.

The compliance guidelines contain five components of what OFAC deems to comprise an effective compliance framework: (i) management commitment; (ii) risk assessment; (iii) internal controls; (iv) testing and auditing; and (v) training. OFAC also provides examples of best practices that companies are expected to follow under each of the five components. With the publication of the new OFAC compliance framework, companies subject to U.S. jurisdiction now have the benefit of a more granular understanding of what policies and procedures will lead OFAC to conclude that their sanctions compliance program is adequate or deficient. The compliance guidelines also describe in detail ten root causes of sanctions violations, including but not limited to the lack of a formal sanctions compliance program; facilitating transactions by non-U.S. persons; exporting or re-exporting U.S.-origin goods, technology or services to OFAC sanctioned persons or countries; and utilizing non-standard payment or commercial practices. We recommend that companies use the OFAC framework as a baseline to assess their own compliance programs, and update them accordingly to reduce the risk of incurring U.S. sanctions liability.

C. New OFAC Transaction Reporting Procedures

On June 21, 2019, OFAC announced an Interim Final Rule amending the Reporting, Procedures, and Penalties Regulations (31 C.F.R Part 501). Notably, the amendment expands the reporting requirements for rejected transactions. Although financial and non-financial institutions alike had previously been required to file blocked property reports, only financial institutions had been required to file rejected transfer reports. Under the new amendment, however, all U.S. persons and persons subject to U.S. jurisdiction are required to submit reports on rejected transactions. The new amendment also makes clear that, in addition to rejected funds transfers, the reporting requirement applies to all rejected transactions, which includes rejected "transactions related to wire transfers, trade finance, securities, checks, foreign exchange, and goods or services." Moreover, the scope of the information to be included in the rejection (and blocking) reports is expanded to include a host of information in order to reduce OFAC's need to issue follow-up requests for additional information.

This new rule materially increases the number of transactions that may need to be reported to the agency; the regulated community and advisors have been engaging with OFAC ever since the announcement to understand the true scope of the transactions that OFAC would like to see reported.

D. New OFAC Penalty Amounts

Also in June 2019, OFAC increased the maximum base penalties for sanctions violations pursuant to the Federal Civil Penalties Inflation Adjustment Act Improvements Act of 2015. This is the fourth time that OFAC has adjusted the applicable civil monetary penalties ("CMPs") since the Act was adopted in 2015.

Under this adjustment, the maximum CMP amount for the five applicable sanctions-related statutes increased as follows:

Statute	Existing maximum CMP amount	Maximum CMP amount effective June 14, 2019
TWEA	$86,976	$89,170
IEEPA	295,141	302,584
AEDPA	77,909	79,874
FNKDA	1,466,485	1,503,470
CDTA	13,333	13,669

Additionally, the OFAC enforcement guidelines published as Appendix A to 31 C.F.R. Part 501 have been updated to reflect these new figures. The update includes a new "base penalty matrix" to assist in calculating possible penalty amounts under the various statutes, which takes into account the egregiousness of the offense and whether the offending transaction was voluntarily disclosed to OFAC:

BASE PENALTY MATRIX

Voluntary Self-Disclosure	Egregious Case: NO	Egregious Case: YES
YES	(1) One-Half of Transaction Value (capped at lesser of $151,292 or one-half of the applicable statutory maximum per violation)	(3) One-Half of Applicable Statutory Maximum
NO	(2) Applicable Schedule Amount (capped at lesser of $302,584 or the applicable statutory maximum per violation)	(4) Applicable Statutory Maximum

E. CAPTA List

On March 14, 2019, OFAC introduced the List of Foreign Financial Institutions Subject to Correspondent Account or Payable-Through Account Sanctions ("CAPTA List"). This list includes identifying information of foreign financial institutions ("FFIs") for whom it is prohibited to open or maintain correspondent or payable-through accounts in the United States under existing legal authorities, including: the Ukraine Freedom Support Act of 2014, as amended by the Countering America's Adversaries Through Sanctions Act; the North Korea Sanctions Regulations; the Iranian Financial Sanctions Regulations; and the Hizballah International Financing Prevention Act of 2015.

Importantly, the CAPTA List is not a new list in its own right; rather, it consolidates information that had previously been included under other lists maintained under various sanctions programs, such as the now-defunct Part 561 List and the (never used) Hizballah Financial Sanctions Regulations List. Notably, entities appearing on the CAPTA List are not included on the SDN List.

Although this list does not contain new information per se, it may prove to be a useful resource for U.S. financial institutions when conducting diligence on FFIs seeking to open correspondent or payable-through accounts in the United States.

IV. Developments in U.S. Export Controls

The Trump administration's practice of using all international trade tools at its disposal to advance its domestic and foreign policy objectives also extended to its use of certain authorities delegated to the U.S. Department of Commerce's Bureau of Industry and Security ("BIS"). Although interagency coordination on sanctions is not new, the Administration's apparent willingness in 2019 to use BIS's export control licensing and enforcement tools to advance its foreign policy and national security interests, including the Administration's trade agenda, was. This was most manifest in BIS's designation of Huawei Technologies Co. Ltd. ("Huawei") to the Export Administration Regulation's ("EAR") Entity List on May 16, 2019, though BIS made frequent use of this and another listing power throughout the year. Importantly, BIS's measures are not technically "sanctions" though they operate in a similar manner and, depending upon the measure, can have similar impacts.

A. Entity List

Entities can be designated to the Entity List upon a determination by the End-User Review Committee ("ERC") that the entities pose a significant risk of involvement in activities contrary to the national security or foreign policy interests of the United States. The ERC is an interagency body with representatives from the Departments of Commerce, State, Defense, Energy, and the Treasury, and which is chaired by Commerce. Through Entity List designations, BIS prohibits the export, re-export, or transfer (hereinafter "export") of specified items to designated entities without BIS licensing. BIS will typically announce either a policy of denial or *ad hoc* evaluation of license requests.

The practical impact of any Entity List designation varies in part on the scope of items BIS defines as subject to the new export licensing requirement, which could include all or only some items that are "subject to the EAR." In addition to items manufactured or exported from the United States, items "subject to the EAR" include (a) foreign-made items containing U.S. content that exceeds the EAR's *de minimis* threshold for controlled content to the country of destination (25% for most countries, 10% for others), (b) certain U.S. content that is exempt from the *de minimis* rule, meaning that any amount of the controlled content will render the foreign-made item subject to the EAR, and to foreign-made items (c) that are the direct product of U.S.-origin technology or software, or (d) that are the products of whole plants or components of plants designed with certain U.S. technology or

software. Those exporting to parties on the Entity List are also precluded from making use of any BIS license exceptions.

Because the Entity List prohibition applies only to exports of items subject to the EAR, U.S. persons are still free to provide many kinds of services and to otherwise continue dealing with those designated in transactions that occur wholly outside of the United States and without items subject to the EAR. While on the one hand, this makes the Entity List prohibition more limited than OFAC's SDN prohibitions, the Entity List prohibition is more extraterritorial in reach because it also prohibits non-U.S. persons from re-exporting or transferring any items subject to the EAR to the listed parties wherever these items are located. OFAC's SDN prohibitions are limited to U.S. person dealings with SDNs, though foreign person dealings with SDNs can be a basis for OFAC's designating the foreign person under certain circumstances.

On May 16, 2019, BIS added Huawei and almost 70 Huawei affiliates to the Entity List. Later, on August 21, 2019, BIS expanded its Huawei designations to include its fabless semiconductor subsidiary, HiSilicon, plus 46 new designations, pushing the total number of Huawei entities designated to over 100. The ERC's cited basis for its original determination was a Superseding Indictment of Huawei filed in the Eastern District of New York which includes among its 13 counts two charges that Huawei knowingly and willfully conspired and caused the export, re-export, sale and supply, directly and indirectly, or goods, technology, and services from the United States to Iran and the Government of Iran without authorization from OFAC.

BIS's prohibition on dealings with Huawei was and continues to be comprehensive; BIS included the export of all items subject to the EAR within the scope of its prohibition and announced that it will review license applications to export to Huawei with a policy presumption of denial. No other company as large as Huawei or with operations in as many countries worldwide had ever been designated by the ERC to the Entity List.

B. BIS Made More Typical Entity List Designations Throughout the Year

On June 24, 2019, BIS designated five Chinese entities involved in exascale high performance computing out of concern that they were developing and using technologies to support nuclear explosive simulation and military simulation activities.

On May 14, 2019, BIS designated twelve entities to the Entity List. Two from China were added due to their role in the unauthorized export of syntactic foam to Chinese state-owned enterprises, defense industrial corporations, and military-related academic institutions. Four more Chinese and Hong Kong entities were added due to their attempts to procure U.S.-origin commodities that would provide material support to Iran's weapons of mass destruction and military programs. A Pakistan entity was added due to its participation in unsafeguarded nuclear activities. Finally, four United Arab Emirates-based entities were designated for their role in procuring U.S.-origin commodities for the SDN Mahan Air and for another entity already identified on the Entity List.

On November 13, 2019, BIS added 22 new entities located in Bahrain, France, Iran, Jordan, Lebanon, Oman, Pakistan, Saudi Arabia, Senegal, Syria, Turkey, the United Arab Emirates, and the United Kingdom. The rationales provided for their designations ran the gamut of U.S. foreign policy concerns. An airline from France was designated for its role in transshipping U.S.-origin items to sanctioned jurisdictions. Entities in Oman, Pakistan, Saudi Arabia, and the United Arab Emirates were designated for their participation in unspecified unsafeguarded nuclear activities, and entities located in Bahrain, the United Arab Emirates, and Turkey were designated for diverting U.S.-origin items to Iran without authorization.

C. One Other Set of Entity List Designations Broke New Ground

and Could Create a Path for Export Control Designations in 2020

While many of BIS's other Entity List designations for the year tracked historical concerns of the United States—for example, nuclear proliferation and sanctions evasion—one set of Entity List designations broke new ground. On October 9, 2019, BIS designated 28 new Chinese entities, including eight major emerging technology companies, for their roles in the implementation of China's campaign of repression, mass arbitrary detention, and high-technology surveillance against Uighurs, Kazakhs, and other members of Muslim minority groups in the Xinjiang Uighur Autonomous Region. While OFAC designations based on human rights concerns have become common in recent years, BIS has not historically used Entity List designations in this way and we anticipate that we will see additional Entity List designations on these grounds in 2020.

V. Legislative Developments: Focus on China

On November 21, 2019, amid mounting tensions between China and Hong Kong over a now-withdrawn extradition bill, the U.S. Congress passed the Hong Kong Human Rights and Democracy Act of 2019 (the "HK Act"), as described in our earlier client alert. The HK Act seeks to protect civil rights in Hong Kong and to deter human rights violations in the territory (including punishing those who commit them). Within a week after the HK Act was passed by supermajorities in both houses of Congress, President Trump signed the HK Act into law on November 27, 2019, despite hinting earlier that he might veto the legislation. An accompanying bill to prohibit the commercial export of covered munitions items to the Hong Kong police force was also signed into law the same day.

The HK Act augments the existing U.S.-Hong Kong Policy Act of 1992 by requiring the U.S. Secretary of State to annually certify to Congress whether Hong Kong retains sufficient autonomy to merit its special trade and investment status. An adverse assessment could potentially threaten this status. Under the HK Act, the President is also empowered to impose sanctions on individuals deemed responsible for human rights violations in Hong Kong. The potential sanctions are varied, and could include asset blocking, which would effectively blacklist any identified party from participating in transactions with U.S. persons, and limit the designated party's ability to engage in U.S. dollar trade (which almost always requires clearing through a bank under U.S. jurisdiction). Other types of sanctions that could be imposed include the revocation or denial of U.S. visas currently issued or to be issued to identified individuals.

China has declared that the HK Act represents an interference in its domestic affairs and has retaliated by announcing sanctions against U.S.-based non-profit organizations, including the National Endowment for Democracy and Human Rights Watch. China also stated that it will prohibit U.S. military vessels from conducting port calls in Hong Kong—though, in practice, such port calls were already typically denied. It remains to be seen if Beijing will impose further retaliatory measures.

On December 3, 2019, the U.S. House of Representatives passed the Uighur Intervention and Global Humanitarian Unified Response Act of 2019 (the "UIGHUR Act") in an attempt to hold Beijing accountable for its alleged human rights abuses against ethnic and religious minorities, particularly the Uighurs (alternatively "Uyghurs") in the Xinjiang region. This bill, which passed by a vote of 407-1, would amend and strengthen a related Senate version of the bill by explicitly linking U.S. policy toward China with the human rights situation in Xinjiang and mandating many of the Senate version's non-binding provisions. In particular, the UIGHUR Act stands to impose a host of sanctions on senior Chinese government officials involved in the human rights abuses towards the Uighurs and implement export controls on U.S.-made items destined for Xinjiang and that could be used by the Chinese government for certain surveillance and repressive activities. If enacted, it would mark the first time that sanctions would be imposed on a member of China's politburo, namely Secretary Chen Quanguo. The Senate now must reconcile and approve the differences between the House and Senate versions, and the President must

sign the final bill for enactment. Key lawmakers have expressed optimism that Congress will be able to move the legislation forward soon, even as concerns about the UIGHUR Act's strengthened export controls provisions and President Trump's impeachment trial may result in delay.

VI. Select U.S. Enforcement

2019 saw OFAC as busy as it has been in over a decade, finalizing 30 cases, assessing record fines, and pursuing novel and aggressive enforcement theories. While OFAC cases are not formally precedential, the agency does use enforcement to educate the public and to indicate OFAC's foremost compliance concerns. In that regard, we provide below an overview of some of the more impactful enforcement actions of the past year.

A. Apollo Aviation

In November 2019, ***Apollo Aviation Group, LLC*** ("Apollo") agreed to pay $210,600 to OFAC to settle its potential civil liability for apparent violations of U.S. sanctions on Sudan. OFAC alleged that Apollo violated U.S. sanctions when it leased three aircraft engines to an entity incorporated in the United Arab Emirates, which then subleased the engines to a Ukrainian airline, who in turn installed the engines on aircraft leased to Sudan Airways. The leases occurred between 2013 and 2015, when Sudan Airways was identified on the SDN List as meeting the definition of "Government of Sudan." The lease agreements that Apollo entered into contained a provision prohibiting the lessee from maintaining, operating, flying, or transferring the engines to any countries subject to U.S. sanctions. However, OFAC alleged that Apollo did not periodically monitor or otherwise verify that the lessee and sublessee were adhering to this lease provision and, as a result, Apollo did not learn that its engines were installed on Sudan Airways aircraft until a review of the engine records after the end of the lease. In determining the appropriate penalty, OFAC considered that Apollo voluntarily self-disclosed the apparent violations, implemented a number of remedial measures in response, and no Apollo personnel had actual knowledge of the conduct leading to the apparent violations.

This case was one of the first to name in an enforcement action a non-operational, private equity investor that did not own the entity at the time of the alleged misconduct. This line of enforcement cases has made it clear that OFAC is increasingly willing to pursue enforcement actions under a theory of successor liability and even against parties not involved in the operational management of an alleged offender.

B. General Electric

In October 2019, the ***General Electric Company*** ("GE"), on behalf of three current and former GE subsidiaries, ***Getsco Technical Services Inc., Bentley Nevada,*** and ***GE Betz*** (collectively, the "GE Companies"), agreed to pay $2,718,581 to settle potential civil liability for 289 alleged violations of U.S. sanctions on Cuba. Specifically, OFAC alleged that between December 2010 and February 2014, the GE Companies accepted 289 payments from The Cobalt Refinery Company ("Cobalt") for goods and services provided to a Canadian customer of GE. Cobalt, an entity owned by a public joint venture between GE's Canadian customer and the Cuban government, has been on the SDN List since June 1995.

Although GE entered into contracts with and issued invoices directly to the Canadian customer, Cobalt paid the invoices in more than 65 percent of the total transactions during the relevant period, with payments totaling approximately $8,018,615. In setting the monetary penalty, OFAC considered the fact that GE identified the alleged violations by testing and auditing its compliance program and then voluntarily self-disclosed the payments to OFAC. This case demonstrated OFAC's continued focus on Cuban violations and the agency's willingness to "pierce the veil" in enforcement cases to find alleged wrongdoing on an indirect basis.

C. British Arab Commercial Bank

In September 2019, ***British Arab Commercial Bank*** ("BACB") agreed to remit $4,000,000 to settle potential violations of the Sudanese Sanctions Regulations stemming from the bank's processing of 72 transactions totaling $190,700,000. OFAC determined that BACB did not make a voluntary self-disclosure and that the violations represented an egregious case, but nonetheless found that the bank's operating capacity was such that it would face disproportionate impact were it required to pay the proposed penalty of over $220 million.

Between September 2010 and August 2014, BACB processed 72 bulk funding payments related to Sudan in relation to its operation of U.S. dollar accounts for at least seven Sudanese financial institutions, including the Central Bank of Sudan. The transactions themselves were not processed to or through the U.S. financial system but the bank did operate a *nostro* account at a non-U.S. financial institution located in a country that imports Sudanese-origin oil to facilitate payments involving Sudan. The bank funded this *nostro* account with large, periodic U.S. dollar wire transfers from banks in Europe, which in turn transacted with U.S. financial institutions in a manner that violated OFAC sanctions. Several BACB employees, including managers and a member of the compliance team, had knowledge of this arrangement. In determining a settlement amount far lower than the potential penalty range, OFAC considered BACB's record free from prior violations, the bank's cooperation with the investigation, and the institution's weak financial position. OFAC also credited BACB for undertaking several remedial measures, including exiting the Sudanese market, hiring new compliance staff and new senior management, and implementing additional compliance procedures.

This case was another in a line of enforcement actions that has seen OFAC continue to extend its theory of jurisdiction, using even an indirect and somewhat attenuated reliance on the U.S. dollar to bring an entire body of transactions under OFAC jurisdiction.

D. Atradius

On August 16, 2019, ***Atradius Trade Credit Insurance, Inc.*** ("Atradius"), a trade credit insurer licensed to operate in the state of Maryland, agreed to pay $345,315 to settle its potential civil liability for two apparent violations of the Foreign Narcotics Kingpin Sanctions Regulations. On May 5, 2016, OFAC designated Grupo Wisa, S.A. ("Grupo Wisa") pursuant to the Kingpin Act and added the entity to the SDN List. In October 2016, approximately five months after Grupo Wisa's designation, a cosmetics company located in the United States assigned to Atradius the right to collect on a debt owed by Grupo Wisa. Atradius subsequently filed a claim in Panama as a creditor in the liquidation of Grupo Wisa, and in June 2017, Atradius received a payment of approximately $4 million from the liquidation of Grupo Wisa's assets in Panama. OFAC alleged that by accepting the assignment of the Grupo Wisa debt, and by receiving the payment from the Grupo Wisa liquidation, Atradius was alleged to have dealt in property or interests in property of a specially designated narcotics trafficker in violation of U.S. sanctions. OFAC considered it an aggravating factor that Atradius did not undertake any meaningful analysis or otherwise seek confirmation from OFAC that assignment of the SDN's debt and acceptance of payment was permissible under existing authorizations.

This enforcement action underlines one of the surprising facts about OFAC designations. Atradius sought to extract money from a sanctioned party, which would presumably be in line with U.S. Government wishes to further harm a designated entity. However, that is not how OFAC sees such dealings. Whether a party is providing a benefit to or attempting to seize payments from a blocked party, it is the dealings with that party that are prohibited. Once on the SDN List, OFAC's desire is to make the party a financial pariah, and almost any engagement requires an OFAC license.

E. DNI and Southern Cross

On August 8, 2019, OFAC issued Findings of Violation to two U.S. companies, ***DNI Express Shipping Company*** ("DNI") and ***Southern Cross Aviation, LLC*** ("Southern Cross"), in relation to administrative subpoenas with follow-up responses deemed by OFAC to be materially inaccurate or incomplete. This is one of the few times OFAC has ever enforced solely on the basis of inadequate responses.

DNI, a shipping company based in Virginia, was under investigation in 2015 for allegedly facilitating the shipment and sale of farm equipment to Sudan in apparent violation of U.S. sanctions. OFAC issued an administrative subpoena and a Cautionary Letter to DNI in May 2015. OFAC determined that DNI, through counsel, demonstrated "reckless disregard" for its U.S. sanctions obligations by providing misleading and inaccurate information in response to a May 2015 administrative subpoena. Similarly, OFAC determined that Southern Cross, a Florida-based aviation company which had been issued an administrative subpoena, demonstrated "reckless disregard" for its U.S. sanctions obligations by failing to provide complete and accurate information in response to OFAC's administrative subpoena, but did consider that the underlying potential sale in question did not appear to have occurred.

F. Paccar Inc.

On August 6, 2019, OFAC announced a $1,709,325 settlement with ***Paccar Inc.*** ("Paccar") to resolve the company's potential civil liability for 63 apparent violations of U.S. sanctions on Iran by ***DAF Trucks N.V.*** ("DAF"), a wholly-owned subsidiary of Paccar headquartered in the Netherlands. Specifically, OFAC alleged that on three occasions between October 2013 and February 2015, DAF sold or supplied 63 trucks to customers in Europe that it knew or had reason to know were ultimately intended for buyers in Iran.

DAF sells its trucks through a network of independent dealers that typically purchase the trucks from DAF and then resell the trucks to identified end-customers. In 2014, a dealer based in Hamburg, Germany requested a price quotation from DAF for 51 trucks with particular specifications for an Iranian company located in Iran. After DAF informed the Hamburg-based dealer that DAF could not sell trucks destined for Iran, the dealer submitted a nearly identical order the same day, this time stating that the trucks were destined for an end-user in Russia. Despite the similarities, DAF did not conduct a further inquiry and processed the order. The dealer then resold the trucks to a buyer in Iran. Separately, in 2013, a directly owned DAF dealer in Frankfurt sold two trucks to a trader based in the Netherlands who in turn resold the trucks to two buyers in Iran, despite receiving draft invoices referencing buyers in Iran. In 2014, DAF sold ten trucks to a dealer in Bulgaria who sold the trucks to an affiliated rental company, which in turn sold the ten trucks to a buyer in Iran. The Bulgarian agent alleged that a DAF employee had introduced its agent to the Iranian buyers. OFAC alleged that in both instances DAF knew or had reason to know that the trucks were intended for Iran.

The Paccar case is a reminder that while most OFAC sanctions programs stop at the water's edge and foreign subsidiaries of U.S. companies do not, as a general matter, come under OFAC jurisdiction, the same is not true under either Iran or Cuba sanctions. In both cases, a foreign subsidiary or affiliate of a U.S. company can find itself subject to the exact same restrictions as their U.S. parent regardless how removed or insulated their activities may appear to be.

G. State Street

In May 2019, OFAC issued ***State Street Bank and Trust Co.*** ("State Street") a Finding of Violation with no accompanying penalty for processing pension payments totaling over $11,000 to a participant who was a U.S. citizen with a U.S. bank account, but who was residing in Iran, a violation of the Iranian Transactions and Sanctions Regulations. Between January 2012 and September 2015, State Street acted as trustee for a customer's employee retirement plan, processing at least 45 pension payments totaling

$11,365 to a plan participant who was a U.S. citizen with a U.S. bank account but who resided in Iran. State Street appeared to have knowledge that the plan participant was a resident of Iran because the beneficiary's address was in Tehran and the bank's sanctions compliance software issued an alert with each payment. The compliance process in place at the time, however, routed such alerts to non-sanctions expert personnel, rather than State Street's sanctions compliance staff. State Street self-reported the violation and modified its process to ensure that such payments are reviewed by its sanctions compliance unit. In issuing a Notice of Violation without a monetary penalty, OFAC considered State Street's self-disclosure of the violation, its remedial action in response to the violation, its screening process in place at the time of the violation, and the fact that no managers or supervisors appeared to have been aware of the conduct that led to the violation.

This matter emphasizes both the expanse of Iran sanctions (applying to any person "ordinarily resident in Iran") while underlining that sanctions expertise within a compliance unit is critical and expected—especially for sophisticated economic actors.

H. Standard Chartered and UniCredit

In a return to the massive bank fines of the past, in April 2019, OFAC announced enforcement settlements against ***Standard Chartered Bank*** ("Standard Chartered") and various UniCredit entities.

Standard Chartered agreed to remit $1.1 billion in a global settlement with federal, state, local, and UK authorities for apparent violations of sanctions programs relating to Burma, Cuba, Iran, Sudan, and Syria. Payment owed to OFAC amounted to $639 million, which was deemed satisfied by payments of penalties assessed by other U.S. federal agencies arising out of the same conduct. OFAC also separately settled a case with Standard Chartered involving violations related to Zimbabwe.

Between June 2009 and May 2014, Standard Chartered processed 9,335 transactions to or through the United States involving persons or countries subject to various comprehensive sanctions regimes administered by OFAC. The total amount processed was $437,553,380. A majority of the conduct related to Iranian-associated accounts maintained in Standard Chartered's Dubai branches, including accounts maintained by a United Arab Emirates-incorporated petrochemical company owned by an Iranian citizen and engaged in the sale of energy products to, from, and through Iran. The Dubai entity processed U.S. dollar transactions to or through the bank's New York branch and other U.S. financial institutions on behalf of customers physically located or ordinarily residing in Iran.

Separately, Standard Chartered agreed to remit $18,016,283 to settle potential civil liability for violations related to Zimbabwe. The bank's New York branch processed 1,795 transactions totaling over $76 million to individuals on the SDN List or parties that were owned 50 percent or more by individuals on the SDN List. OFAC determined that Standard Chartered voluntarily self-disclosed these apparent violations and that they constituted a non-egregious case. OFAC also identified several failures in the bank's compliance program including insufficient procedures to identify and "ring-fence" SDN customers, but also credited Standard Chartered's cooperation with the investigation.

OFAC announced three separate settlements totaling $611 million with three UniCredit Group banks, including ***UniCredit Bank AG*** (Germany), ***UniCredit Bank Austria AG*** (Austria) and ***UniCredit S.p.A.*** (Italy), resolving its investigation into apparent violations of a number of U.S. sanctions programs. UniCredit Bank AG in Germany agreed to remit $553,380,759 to settle its potential civil liability; UniCredit S.p.A., the parent company of the UniCredit Group, and UniCredit Bank Austria AG agreed to remit a total of $57,542,662 to settle potential civil liability.

While these penalties were substantial, they do not necessarily portend another surge in sanctions enforcement against financial institutions. Notably, the apparent violations date back a decade or more, suggesting that these are legacy actions rather than an indication of future enforcement priorities. However, these matters demonstrate that OFAC remains ready, willing, and able to impose massive fines on global institutions.

I. Kollmorgen

In February 2019, ***Kollmorgen Corporation*** ("Kollmorgen"), on behalf of its Turkish affiliate, ***Elsim Elektroteknik Sistemler Sanayi ve Ticaret Anonim Sirketi*** ("Elsim"), agreed to remit $13,381 to settle potential civil liability for six apparent violations of U.S. sanctions on Iran. Specifically, OFAC alleged that between July 2013 and July 2015, Elsim appeared to violate U.S. sanctions on Iran when, on six occasions, Elsim serviced machines containing Elsim products located in Iran and provided products, parts, or services with knowledge they were destined for Iranian end-users.

OFAC determined that despite Kollmorgen's extensive compliance efforts, a monetary penalty remained appropriate due to Elsim's egregious conduct and specific risk profile, including that Elsim had previously engaged in business with Iran. Notably, OFAC sanctioned a Turkish national employee, Evren Kayakiran, for directing the apparent violations and his attempted concealment of them. The action against Kayakiran is the first time OFAC has named an individual a Foreign Sanctions Evader in relation to a civil enforcement action. This demonstrates an additional, very serious consequence that can emerge from an enforcement action—it is not just a penalty and compliance obligations, but individuals directly involved can actually end up blacklisted.

J. e.l.f. Cosmetics

In January 2019, ***e.l.f. Cosmetics, Inc.*** ("ELF") agreed to pay $996,080 to settle its potential civil liability for 156 apparent violations of U.S. sanctions on North Korea. Specifically, OFAC alleged that between April 2012 and January 2017, ELF imported false eyelash kits from two suppliers located in the People's Republic of China that contained materials sourced from North Korea. This case has been interpreted to demonstrate OFAC's growing concern about supply chain management, and especially some jurisdictions (like North Korea's) willingness to co-mingle commodity supply chains.

During the operative time period, OFAC alleges that ELF's OFAC compliance program was either non-existent or inadequate. The company and its supplier audits failed to discover that approximately 80 percent of false eyelash kits supplied by the two China-based suppliers contained materials sourced from North Korea until January 2017. Subsequently, OFAC determined that ELF voluntary self-disclosed the apparent violations to OFAC and that the apparent violations constitute a non-egregious case.

In determining the penalty amount, OFAC considered among other factors the fact that ELF's personnel did not appear to have had actual knowledge of the conduct at issue and that the apparent violations did not appear to constitute a significant part of ELF's business activities. Further, OFAC considered the company's cooperation with OFAC by immediately disclosing the apparent violations, signing a tolling agreement, and submitting a complete and satisfactory response to OFAC's request for additional information.

In addition to the OFAC enforcement actions, this overview would not be complete without referencing an enforcement action that, via an unprecedented judicial action, was overturned in *Exxon Mobil Corp. v. Mnuchin*.

On December 31, 2019, the U.S. District Court for the Northern District of Texas vacated a $2 million final penalty notice issued by OFAC to ***Exxon Mobil Corporation*** ("Exxon"),

finding that OFAC had failed to provide fair notice that Exxon's entry into contracts with Rosneft that were signed by Rosneft CEO Igor Sechin, an SDN, would violate sanctions rules.

Igor Sechin was added to the SDN List in April 2014 under Executive Order 13661 relating to Russian activities in the Crimea region of Ukraine. The next month, Exxon entered a series of contracts with its existing business partner Rosneft. The contracts were signed by Sechin acting in his representative capacity as chief executive of Rosneft. OFAC issued an administrative subpoena to Exxon and, following an investigation, issued a penalty notice to Exxon imposing a $2 million fine.

Exxon objected and filed suit. The court considered whether OFAC had carried its burden of providing "fair notice" to the public regarding its interpretation of Executive Order 13661 and related implementing regulations. A "Frequently Asked Question" ("FAQ") posted on OFAC's website under the Burma sanctions program announced the agency's interpretation that U.S. persons could not enter into contracts signed by an SDN, even if the company represented by the SDN was not itself blocked. However, similar FAQs for the Ukraine program were not published until after Exxon had signed the contracts. In addition, various White House Factsheets and other executive branch public statements had emphasized that the sanctions targeted the designated persons "individually" and with respect to their "personal assets." The court concluded that a regulated party "acting in good faith" would not have known with "ascertainable certainty" that Sechin's signature on the contract would constitute a prohibited receipt of a service from an SDN.

VII. European Union Legislative Developments, Enforcement and Judgements

In 2019, the European Union became more active in addressing EU common foreign and security policy ("CFSP") objectives with the help of what it calls "restrictive measures," i.e., EU financial and economic sanctions. This included targeting new issues that had not been precisely addressed by "traditional" EU sanctions. For example, the EU imposed a new sanctions framework for responding to cyber-attack threats. Further "new" types of EU sanctions are under discussion, such as EU human rights-related, "Magnitsky-like" sanctions. The EU has also become more vocal on how it expects individuals and companies under its jurisdiction to implement EU sanctions. For instance, the bloc issued unprecedented detailed guidance regarding how to comply with the EU Blocking Statute. Furthermore, the EU has published guidance on internal compliance programs for dual-use trade controls.

We have discussed these developments and respective challenges in depth in our recently published treatise *U.S., EU, and UN Sanctions: Navigating the Divide for International Business*. Below, we provide an update on the most recent developments.

A. EU Legislative Developments

With the recent start of Ursula von der Leyen's term as the new President of the European Commission, the EU has already been active on the topic of sanctions: "The EU Commission emphatically rejects sanctions against European companies that engage in projects in line with the law," von der Leyen noted in response to U.S. sanctions against EU companies working at finalizing the Nord Stream 2 pipeline. Further, without yet providing details, von der Leyen has discussed sanctions as a means to resolve trade disputes, saying "[w]e must ensure that we can enforce our rights, including through the use of sanctions, if others block the resolution of a trade conflict." We expect EU sanctions to play a key role in addressing and enforcing the CFSP and potentially also to be applied in trade disputes in the years to come.

Additionally, several EU member state foreign ministers have requested a reform of the EU sanctions regime, specifically asking for faster implementation of, better guidance on,

and stricter compliance with EU sanctions. We expect further development on this front.

1. EU Human Rights Sanctions

On December 9, 2019, the EU agreed to begin the necessary preparatory work to develop a global sanctions regime to address serious human rights violations. Josep Borrell, the EU's High Representative for Foreign Affairs and Security Policy, noted that the legislation will be the "Magnitsky Act of the EU." In line with some media reports, we expect the EU human rights sanctions to take several months before taking effect.

2. Cyber-Attack Threats

The EU took a step forward in demonstrating its determination to enhance the EU's cyber-defense capabilities with the introduction, on May 17, 2019, of a new sanctions framework in response to cyber-attack threats (as discussed in detail in our recent client alert.) The announced framework creates restrictive measures to deter and respond to cyber-attacks that constitute an external threat to the EU or its member states.

The framework is significant for two reasons. First, it enables the EU to implement unilateral cyber sanctions—a move that expands the EU's sanctions toolkit beyond traditional areas of sanctions, such as sanctions imposed in response terrorism and international relations-based grounds.

Second, it represents a major, concrete measure that arose out of the EU's continued interest in developing an open and secured cyberspace and amid concerns about the malicious use of information and communications technologies by both state and non-state actors. From the alleged plot by Russia to hack the Organization for the Prohibition of Chemical Weapons in The Hague in April 2018 to a cyber-attack on the German Parliament, European leaders have been very concerned about future cyber-attacks on EU member states.

B. EU Economic Sanctions & EU Dual-Use Regulation Updates

Council Regulation (EC) 428/2009—regularly referred to as the EU Dual-Use Regulation—has established an EU regime for the control of export, transit, and brokering of dual-use items in order to contribute to international peace and security by precluding the proliferation of nuclear, chemical, or biological weapons and their means of delivery. In the interplay with EU economic sanctions and national EU member state export laws, it forms part of what one could refer to as "EU Export Controls."

To adapt to rapidly changing technological, economic, and political circumstances, the EU Commission presented a proposal in September 2016 to update and expand the existing rules that was supported by the European Parliament in its first report on the matter. On June 5, 2019, the Council issued its own parameters for negotiations with the European Parliament seeking a more limited recast of the dual-use regulation. Thereby the discussion mainly focuses on the classification of cyber surveillance technologies as dual-use goods and the possibility of a resulting discrimination of EU companies. The progress of the respective discussions can be viewed at the respective EU legislative train.

The respective legislative train has not yet reached the station, and it remains to be seen whether it will be a priority of von der Leyen's.

However, the EU Commission already started to become more vocal on how it expects individuals and companies under its jurisdiction to implement EU sanctions. We summarized key recommendations of this new EU guidance and some additional points we consider helpful in our recent client alert.

Taking into account both the new EU guidance and the Framework for OFAC Compliance Commitments, there is a clear trend from authorities to articulate in detail their expectations on how companies should address sanctions and export control compliance. In turn, it can be expected that non-compliance with such expectations will increasingly be under enhanced regulatory scrutiny.

Further, EU member states have indicated that they might have additional, independent expectations. For instance, the Netherlands has issued its own set of guidelines for companies to assist with establishing an internal compliance program for "strategic goods, torture goods, technology and sanctions."

1. Iran

Following the implementation of the JCPOA in January 2016, most nuclear-related EU financial and economic sanctions were removed. However, several prohibitions and authorization requirements remain in place, specifically with respect to prohibited support for Iran's ballistic missile program.

Furthermore, since 2011, the EU has adopted and regularly renewed non-nuclear Iran financial and economic sanctions related to violations of human rights, including asset freezes and visa bans for entities and individuals responsible for grave human rights violations and a ban on exports of equipment that might be used for internal repression or for monitoring telecommunications. These measures were last extended on April 8, 2019 until April 13, 2020.

In response to the U.S. decision to abandon the JCPOA, on August 6, 2018 the European Union enacted Commission Delegated Regulation (EU) 2018/1100 which amended the EU Blocking Statute. The EU Blocking Statute is a 1996 European Commission Regulation (No 2271/96) which was designed as a countermeasure to what the EU considers to be the unlawful effects of third-country (primarily U.S.) extraterritorial sanctions on "EU operators." The combined effect of the EU Blocking Statute and the Re-imposed Iran Sanctions Blocking Regulation, *inter alia*, is to prohibit compliance by EU operators with U.S. sanctions that have been re-imposed following the U.S. withdrawal from the JCPOA. Further, decisions rendered in the United States or elsewhere because of the sanctions blocked by the EU Blocking Statute cannot be enforced in the EU. Finally, the EU Blocking Statute allows EU operators to recover damages arising from the application of the extraterritorial measures and requires EU operators to report to the EU.

Two principal trends have emerged after the end of the first full year of an "active" EU Blocking Statute. While enforcement by the competent authorities of the EU member states has been limited, the EU Blocking Statute has not been the paper tiger some have suggested; an interesting feature of the landscape over the last year has been private enforcement of the EU Blocking Statute by parties to commercial litigation before the domestic courts of the EU member states. In a number of instances, non-EU companies, including Iranian companies, have relied on the EU Blocking Statute to secure enforcement through the national courts of EU member states of contracts relating to sanctioned countries against EU companies refusing performance by reference to the extraterritorial effects of U.S. sanctions.

Furthermore, Instex was established in January 2019 by France, Germany, and the United Kingdom to facilitate non-U.S. dollar and non-SWIFT trade with Iran. While additional EU member states became shareholders of the French incorporated vehicle, it substantially fell behind expectations.

The recent escalation in tensions between the United States and Iran led President Trump to renew his call for the remaining parties to the JCPOA to abandon the deal and re-introduce EU Iran nuclear-related sanctions.

While EU leaders have opted to rally behind the JCPOA, ignoring the U.S. administration's repeated calls to abandon the agreement, this should not be seen as an indication that the EU would not be willing to reintroduce EU Iran nuclear-related sanctions in the event that Iran does not uphold its part of the bargain. UN Security Council Resolution 2231 (2015), which endorsed the JCPOA, includes a "snapback" mechanism that would be triggered and eventually lead to the reintroduction of UN and EU nuclear-related Iran sanctions if the International Atomic Energy Agency, the UN's nuclear watchdog, were to find Iran was no longer complying with the terms of the JCPOA.

In its latest statements in response to the killing of General Soleimani, Iran has threatened to no longer observe the JCPOA's limitations of centrifuges—a key commitment under the JCPOA. The French, German, and UK foreign ministers responded by issuing a statement and referring the matter to the JCPOA dispute resolution mechanism. While Iran still has the opportunity to change its course of action, it is possible that this statement has triggered the last chapter of the JCPOA. As of today, 2020 might see a "snapback" of UN and EU nuclear-related sanctions.

2. Cuba

As discussed above, the increased U.S. sanctions pressure on Cuba has received broad resistance within the EU. The EU Blocking Statute already applies to Titles I, III, and IV of the Helms-Burton Act. Accordingly, the restrictions apply to this most recent set of U.S. Cuba sanctions. According to Article 4 of the EU Blocking Statute, any judgment enforcing the laws listed in the annex, including Helms-Burton, cannot be recognized or enforced in any EU member state. This means that the doctrine of *res judicata* (the Latin term for "a matter [already] judged") no longer applies in these instances.

Further, the EU Blocking Statute not only prohibits EU operators from complying with Helms-Burton but also entitles them to recover any damages, including legal costs, caused by the application of the law. Indeed, the EU Blocking Statute might also be used as a "clawback" mechanism of any damages that may be awarded in a Title III action. As noted, no cases under Helms-Burton have yet been finalized and consequently this aspect of the EU Blocking Statute remains untested.

Additionally, it is important to take into account national, and specifically EU member state, anti-boycott (anti-declaration) provisions, particularly those relating to Cuba.

As an example, for transactions, individuals and entities subject to German jurisdiction, Section 7 of the German Foreign Trade and Payments Ordinance (Außenwirtschaftsverordnung ("AWV")), states that "[t]he issuing of a declaration in foreign trade and payments transactions whereby a resident participates in a boycott against another country (boycott declaration) shall be prohibited." This originally had to be read with the implicit addendum "to the extent such a declaration would be contradictory to UN, EU and German law." Accordingly, any compliance advice included the burdensome task of understanding the specific extent of applicable UN, EU, and German sanctions and export control rules.

If an individual or entity was understood to declare that it was in compliance with specific U.S. sanctions against, *inter alia*, Cuba and Iran that were not mirrored by the UN, the EU, or Germany, such a declaration was regularly covered and thus prohibited by Section 7 AWV. If the German Public Prosecutor wanted to pursue such a case, a court could find the individual or entity to be in breach of Section 7 AWV, which could then lead to an administrative penalty of up to €500.000 (per declaration) for both the company and the acting employee. Further, it could also lead to forfeiture of income associated with the declaration, (partial) nullity of the provision in respective contractual arrangements, and reputational damages.

On December 19, 2018, Section 7 AWV was amended, adding a provision that a

declaration of a boycott against another state is excluded from Section 7 AWV prohibitions if the UN, the EU, or Germany have issued economic sanctions against that state as well. After such a change, the general view is that it is permitted under German law to declare compliance with a boycott against another country if the UN, the EU, or Germany have imposed any sanctions (regardless to what extent) on the particular country.

Accordingly, individuals and entities may now lawfully declare their intent to comply with U.S. sanctions, at least under Section 7 AWV, if the UN, the EU, and/or Germany have also imposed economic sanctions against that particular state. This is the case with Iran, for example, where UN, EU, and German sanctions are in place. While the dilemma of complying with either U.S. sanctions or the EU Blocking Statute remains, the EU Blocking Statute currently only covers certain sanctions of the United States. Therefore, while it is still important to tailor such statements (usually appearing in representations and warranties) carefully, a broader statement of compliance with U.S. sanctions on Iran has become permissible under German law. With respect to Cuba (or Israel or any other country not in the scope of UN, EU, and/or German sanctions), Section 7 AWV continues to apply.

3. North Korea

While 2018 gave rise to significant new and partly autonomous EU economic and financial sanctions against North Korea due to the deteriorating security situation on the Korean peninsula and regular threats by Kim Jong Un to attack South Korea or the United States, in 2019 the EU mostly maintained the scope of its sanctions on North Korea. The EU did, however, revise its lists of North Korea-related designated parties, which now consist of 57 individuals and 9 entities.

4. Venezuela

The EU Venezuela sanctions include an arms embargo as well as travel bans and asset freezes on listed individuals, targeting those involved in human rights violations and those undermining democracy or the rule of law. On September 27, 2019, the European Council added 7 members of the Venezuelan security and intelligence forces to the list of designated individuals, now including 25 listed persons. On January 9, 2020, the EU's High Representative, Josep Borrell, declared that the EU is "ready to start work towards applying [additional] targeted measures against individuals" involved in the recent use of force against Juan Guaidó, the president of Venezuela's National Assembly, and other lawmakers to impede their access to the National Assembly on January 5, 2020. The EU Venezuela sanctions have recently been extended until November 14, 2020.

5. Syria

EU Syria economic sanctions include an oil embargo, certain investment restrictions, asset freezes applying to the Syrian central bank, as well as export restrictions on equipment and technology used to monitor or intercept telecommunications or for internal repression. EU Syria financial sanctions include travel bans and asset freezes for persons involved in violently repressing the civilian population in Syria, benefiting from or supporting the regime, or being associated with such persons or entities. Currently 269 individuals and 69 entities are designated under the EU Syria sanctions program. On May 17, 2019, the EU extended its sanctions against the Syrian regime for one year, until June 1, 2020.

6. Russia and Crimea

As discussed in previous client alerts, since March 2014, the EU has progressively imposed economic and financial sanctions against Russia in response to Moscow's deliberate destabilization of Ukraine and its annexation of Crimea. EU economic sanctions against Russia continue to include an arms embargo; an export ban on dual-use goods for

military use or military end-users in Russia; limited access to EU primary and secondary capital markets for major Russian state-owned financial institutions and major Russian energy companies; and limited Russian access to certain sensitive technologies and services that can be used for oil production and exploration. However, there are certain noteworthy differences between U.S. and EU sanctions targeting Russia and the latest U.S. actions against Russia have created further disparities between the two regimes.

Further, the EU still does not recognize the annexation of Crimea and Sevastopol by Russia, and the EU imposed broad sanctions against these territories in 2014. The EU Crimea sanctions include an import ban on goods from Crimea and Sevastopol; broad restrictions on trade and investment related to certain economic sectors and infrastructure projects in Crimea and Sevastopol; an export ban on certain goods and technologies to Crimea and Sevastopol; and a prohibition to supply tourism services in Crimea or Sevastopol.

The EU economic sanctions against Russia have been renewed and are currently in place until July 31, 2020. Also, the EU financial sanctions were further extended in September 2019 until March 15, 2020. As of now, 170 people and 44 entities are subject to a respective asset freeze and travel ban. On June 20, 2019, the European Council also extended the EU Crimea sanctions until June 23, 2020. These restrictions are similar to those in place in the United States.

We expect the EU Russia and Crimea sanctions to stay in place for the time being. High Representative Borrell has previously indicated that he believes that “[u]ntil such time as Russia changes its attitude on Crimea and territorial violations, those [EU Russia] sanctions must remain.”

Finally, given how upset the EU has been regarding recent U.S. sanctions on Nord Stream 2, it would be logical to assess that the EU Blocking Statute could be extended to include the NDAA, which provides for targeted sanctions on Nord Stream 2. The EU Blocking Statute currently does not apply to U.S. Russia sanctions. However, we think this outcome is unlikely. The EU Trade Commissioner, Phil Hogan, pointed out that the EU opposes sanctions generally if they threaten companies involved in legitimate business. European Commission President Ursula von der Leyen stated, “The EU Commission emphatically rejects sanctions against European companies that engage in projects in line with the law.” Overall, the EU authorities appear to be at least momentarily satisfied that the U.S. sanctions are unlikely to actually be implemented in this late stage of the construction process, even if they are perceived as an “unfriendly act.”

7. Turkey

Considering that Turkey remains an official applicant for EU membership, it was a surprising development for the bloc to establish on November 11, 2019 an EU financial sanctions framework targeting Turkey’s drilling for natural resources off the coast of Cyprus. The contemplated EU financial sanctions include travel bans and asset freezes. So far, no entity has been designated under the new EU Turkey sanctions. EU Turkey sanctions are aimed at deterring Ankara from violating Cyprus’s maritime economic zone by drilling off the coast of the divided island. In a separate decision, the EU also imposed an arms embargo prohibiting new arms sales by EU member states to Turkey in light of Turkey’s involvement in the Syria conflict.

8. Saudi Arabia

After the assassination of dissident journalist Jamal Khashoggi at the Saudi consulate in Istanbul in October 2018, the German Federal Government issued a unilateral moratorium on arms exports to Saudi Arabia. While originally aligned with France and the United Kingdom, the moratorium did not take the form of EU economic sanctions. Rather, the competent German authority stopped issuing necessary export licenses, including for

exports that had previously been approved by the German government.

The Administrative Court of Frankfurt am Main has now lifted this *de facto* export ban, at least with respect to a specific request to ship an arms manufacturer's trucks. According to the court, the specific case was about 110 unarmored vehicles for the Royal Saudi Land Forces. The export of the trucks had been authorized in 2017, and 20 vehicles had then been delivered by the end of October 2018. With an order dated November 2018, the Federal Office of Economics and Export Control (Bundesamt für Wirtschaft und Ausfuhrkontrolle ("BAFA")) temporarily "suspended the validity of the authorization." Subsequently, additional orders with extended temporary suspensions were issued. After the BAFA failed to respond to the company's complaint, the company brought an action for failure to act.

It is noteworthy that the question of whether or to what extent EU member states are free to unilaterally (i.e., without alignment with other EU member states) introduce national sanctions measures, such as an asset freeze, has been the topic of a broader recent debate in the EU. The European Commission has published a non-binding opinion in response to a request by an EU member state national competent authority on the compatibility of national, unilateral asset-freezing measures with EU law. According to the opinion, a unilateral asset freeze measure, such as those regularly imposed by EU financial sanctions, are generally not permissible if based on grounds covered by Article 215 of the Treaty on the Functioning of the European Union.

9. Nicaragua

On October 14, 2019, the EU adopted a legal framework for EU financial sanctions targeting Nicaragua, including travel bans and asset freezes against individuals and entities that have committed human rights violations or abuses, repressed civil society and democratic opposition, or undermined democracy and the rule of law in Nicaragua. Furthermore, EU individuals and entities also will not be allowed to make funds available to listed individuals and entities. So far, no designations have been made.

10. Myanmar/Burma

On April 29, 2019, the EU extended EU economic sanctions on Myanmar/Burma for one year, until April 30, 2020.

The EU economic sanctions against Myanmar/Burma include an embargo on arms and equipment that can be used for internal repression, an export ban on dual-use goods to be used by the military and border police, as well as restrictions on the export of equipment for monitoring communications that might be used for internal repression. Furthermore, the provision of military training to and military cooperation with the Myanmar Armed Forces (Tatmadaw) is prohibited under the sanctions regime.

The extension of the EU financial sanctions includes restrictive measures imposed on 14 officials of the Tatmadaw and the border police for human rights violations or association with such violations.

VIII. EU Member State Enforcement Action and Judgements

Enforcement of EU financial and economic sanctions takes place at the EU member state level. Judgments regarding EU financial and economic sanctions also regularly take place at the EU member state level. However, the EU's supranational courts may be called upon to address specific questions and hold jurisdiction over particular matters, such as de-listing requests.

A. Belgium

In February 2019, the Antwerp Criminal Court found three Belgian companies and two of their managing directors guilty of violating EU Syria sanctions for exporting chemicals to Syria without the necessary license. The court imposed fines between €75,000 and €500,000 on ***AAE Chemie Trading*** ("AAE"), ***Anex Customs*** ("Anex"), and ***Danmar Logistics*** ("Danmar") for creating a supply chain to export the chemicals to Syria. AAE's managing director was given a conditional fine of €346,000 and received a four-month conditional sentence, and Anex and Danmar's managing director was given a conditional fine of €500,000 and was sentenced to a 12-month custodial sentence.

B. Denmark

In September 2019, Danish state prosecutors started investigating ***Dan-Bunkering***, the Danish bunker fuel supplier, on suspicion of violation of the EU Syria sanctions. According to U.S. court records and public sources, Dan-Bunkering was involved in supplying at least 30,000 metric tons of jet fuel for the civil war in Syria. According to Russia's Foreign Ministry, the company that ordered the supplies was in charge of supplying fuel for Russian fighter jets conducting air raids in Syria. A confidential report submitted to the court detailed transactions totaling DKK 342 million (approximately $50 million) between Dan-Bunkering and the Russian company Maritime in 2016 and 2017.

C. Estonia

In autumn 2019, Estonia started taking measures against the news agency ***Sputnik Estonia*** in order to implement EU sanctions. Sputnik Estonia is controlled by Russia Today, the Russian state media organization. Dimitry Kiselyov, the head of Russia Today, is on the EU's list of those subject to an asset freeze and travel restrictions for their involvement in "undermining or threatening the territorial integrity, sovereignty and independence of Ukraine." Because of this, Estonian officials took enforcement measures against Sputnik Estonia.

At the end of October 2019, Estonian branches of foreign banks stopped payments by Sputnik Estonia, thus making the payment of salaries, taxes, and rent impossible. As a consequence, Sputnik Estonia received a termination notice from its landlord. In December 2019, the employees of Sputnik Estonia received a warning from the Estonian Finance Intelligence Unit informing them of possible criminal liability if they continued to work for Sputnik Estonia. Subsequently, all 35 employees of the news agency resigned. In December 2019, Sputnik Estonia announced that it would be closing its operations in Estonia.

D. France

In April 2019, the Sanctions Committee of the French Banking Regulator opened disciplinary proceedings against the bank ***Raguram International*** for shortcomings in its screening of customers with regard to sanctions compliance. No penalty was issued due to the ensuing compliance efforts by the bank.

E. Germany

1. Russia Arms Embargo

The Hamburg Higher Regional Court sentenced a Russian citizen to seven years in prison for violating European sanctions by selling sensitive dual-use technology worth over €1.83 million to Russians with military backgrounds between 2014 and 2018. In doing so, this individual both forged the necessary documents and violated the export ban under Council Common Position 2008/944/CFSP. He sold, among other things, two hot isostatic presses. As these can be used for civilian or military purposes, exporting them to Russia is prohibited. He further sold up to 15 kilograms of decaborane chemicals, also to a Russian

military recipient. The chemicals can be used as rocket fuel or explosives. The items, which can be used for military purposes, fall under the EU Russia economic sanctions.

2. Mahan Air

In January 2019, Germany revoked the license of Iranian airline Mahan Air, which Germany alleged was transporting military equipment and personnel to Syria and other Middle East war zones. The airline is subject to U.S. terrorism secondary sanctions imposed in 2011 for its support for the IRGC. Partly in response to pressure from the United States, Germany imposed the sanctions on Mahan Air after discovering a spy working as a translator in the Bundeswehr.

IX. United Kingdom

2019 saw the United Kingdom's Office of Financial Sanctions Implementation ("OFSI") impose its first monetary penalties pursuant to the Policing and Crime Act 2017 ("PCA"). OFSI has the authority to substitute a criminal prosecution with a civil monetary enforcement for breaches of financial sanctions legislation. The maximum penalty a company can receive pursuant to the PCA is the greater of either £1 million (approximately $1.3 million) or 50% of the approximate value of the funds or the economic resources provided.

Guidance provided by OFSI in May 2018 highlights the factors to be considered when calculating the potential for, and amount of, the monetary penalty that may be levied. A number of these factors mirror those applied in other compliance regimes, including whether the breach was systemic, the level of knowledge within the organization, whether funds were provided directly, or actions were taken to circumvent the sanctions, etc.

A. House of Commons - Foreign Affairs Committee Report, and Government Response

On June 12, 2019, the Foreign Affairs Committee of the House of Commons published a scathing report (the "Report") in relation to the UK's sanctions regime post-Brexit and preparations in relation thereto. The Report, entitled "Fragmented and incoherent: the UK's sanctions policy," highlighted three key elements of sanctions policy that the Committee considered had been overlooked including: (i) a clear high-level Government strategy; (ii) an effective structure for cross-governmental coordination; and (iii) an acknowledgment of the overlap between sanctions and anti-money laundering enforcement in practice.

The overall strategy deficiencies included concern over the timing of incorporation of EU sanctions legislation into local law, a lack of legal certainty regarding whether, and when, the UK will be able to implement and use "Magnitsky-style" powers (that is to say, sanctions targeting human rights violators), and an absence of clarity regarding post-Brexit cooperation with the EU.

In order to overcome some of the deficiencies in the policy making and enforcement structures, the Report recommended the appointment of a Senior Responsible Officer ("SRO") who would be personally accountable to the National Security Council in relation to sanctions policy and enforcement. The Report further recommended consideration be given to the creation of a single body with responsibility for both policy and enforcement, along the lines of OFAC in the United States.

Finally, while acknowledging that sanctions and anti-money laundering policy are distinct, the Report recommended a greater appreciation by the Foreign and Commonwealth Office ("FCO") of the overlap between the two, using the example of the listing of En+ Group on the London Stock Exchange in 2017 as a failure in practical enforcement due to the

sanctions laws in force at the time being too narrow to effectively block such a listing, and there being no clear way for the Financial Conduct Authority ("FCA") to convey its concerns or consult national security experts. The Report also re-iterated its previous recommendation for there to be an assessment of the effectiveness of OFSI. The overall conclusion of the Report was that "the Government has spent the last two years running as fast as it can just to stay in the same place."

The Government's response (the "Response") to the concerns raised by the Report was published on September 3, 2019. The Response began by noting the complexity, and unique and dynamic nature of the 22 statutory instruments that had to be drafted in order to translate EU sanctions into local law. The Government also noted that this in turn utilized unprecedented resources and time.

The Response indicated that post-Brexit the Government intends to implement Magnitsky-style sanctions as well as publish its own designated persons list to facilitate enforcement of the same. The Response confirmed the Government's hope to continue international cooperation in relation to its sanctions regime while maintaining independent policy-making and using its permanent seat on the UN Security Council to express and coordinate the imposition of international sanctions.

In response to the Report's more domestic concerns, such as its suggestion to appoint an SRO, the Government confirmed that it already has multiple SROs within the FCO, and will re-assess the need for a single SRO designation in the future. Additionally, the Response considered the Report's concern regarding permission for En+ to list on the London Stock Exchange, the Government re-iterated that the FCA is an independent body, and is empowered under the Financial Services and Markets Act 2000 to refuse an application for listing where it would be detrimental to the investor. Furthermore, the Government stated that it is deliberating the possibility of introducing a power to block a listing on grounds of national security to overcome such challenges in the future.

In relation to the wider consideration of the overlap between sanctions and anti-money laundering efforts, the Government confirmed that its intention is to keep the two separate, however it recognized the overlap and highlighted the systems existing alongside sanctions in the Government's artillery to fight economic crime. Lastly, the Government defended the effectiveness of OFSI, noting its success in communicating the latest sanctions, its guidance in relation to sanctions compliance, and the threat of monetary enforcement being a strong deterrent.

B. Enforcement

1. R. Raphael & Sons plc

In January 2019, OFSI issued its first financial penalty, against UK bank ***Raphael & Sons plc*** ("Raphaels Bank"), of £5,000, for dealing with funds belonging to a designated person without a license, in contravention of regulation 3 of the Egypt (Asset-Freezing) Regulations 2011 (S.I. 2011/887). The value of the transaction at issue was £200. Raphaels Bank made a disclosure of the transaction to OFSI and cooperated with the regulator which resulted in a reduction in penalty of 50 % from an initial fine of £10,000.

2. Travelex (UK) Ltd

OFSI issued its second enforcement in May 2019 against ***Travelex (UK) Ltd.*** for contravention of regulation 3 of the Egypt (Asset Freezing) Regulations 2011 (S.I. 2011/887) by dealing with funds belonging to a designated person without a license. This breach was linked to the penalty imposed against Raphaels Bank. OFSI found that "Travelex had direct, in-person, contact with a designated person (DP), in the UK, and dealt with funds belonging to that person despite having access to their passport, which clearly identified the individual by name, date of birth and nationality." The transaction in

question was valued at £204, however no discount was applied for voluntary disclosure and therefore the company was fined £10,000.

3. Telia Carrier UK Limited

OFSI's largest monetary penalty yet was levied against ***Telia Carrier UK Limited*** ("Telia"), a UK subsidiary of Telia Company on October 28, 2019. Telia was fined for breaching section 4 and 6 of the Syria (European Union Financial Sanctions) Regulation 2012. SyriaTel, the sanctioned entity, is the largest mobile phone company in Syria and is owned and controlled by Rami Makhlouf, a powerful Syrian businessman and cousin of President Bashar al-Assad. The company was designated in 2011 by both the United States and the EU, and was described as "being controlled by one of the regime's most corrupt insiders." The decision from OFSI while not detailed, confirmed that the telecom carrier's facilitation of international telephone calls to SyriaTel involved "repeatedly making economic resources available to the designated entity over an extended period of time." OFSI took the opportunity to remind businesses of the broad scope of assistance that it would consider providing "economic resources," including tangible and intangible assets that can be transferred either directly or indirectly. This broad definition is likely to be of interest to global businesses in all sectors. The decision confirmed that OFSI's investigation found that the company "had knowledge, or had reasonable cause to suspect it was breaching sanctions." The regulator urged companies to implement more thorough screening processes and self-report when issues are identified.

Interestingly, this is the first OFSI enforcement in which the ministerial review process, as provided for in Section 147 of the PCA, was engaged and the penalty in this matter was reduced substantially after the review. When ministerial review is requested by a company, there are three potential outcomes: (i) upholding the decision to impose a penalty and the amount; (ii) upholding the decision to impose a penalty but changing the amount; and (iii) canceling the decision to impose any penalty. The Guidance provided by OFSI in May 2018 confirms that a party requesting a review has 28 days to do so from the date on which it receives written confirmation of the penalty. Once a review is requested, no new material is generally required and this process is not designed to be an opportunity to introduce new evidence. However, in this case, during the review process, OFSI received further clarification regarding the nature of the transactions which it did not have when deciding the initial penalty. As a result the assessed value of the transactions was more than halved from £480,000 to £234,000. OFSI noted that this information needed to be considered even though it was provided as such a late stage, given the "significant impact" of the information. While it is unclear what would be considered "significant impact" and therefore what information will be of assistance to OFSI, companies found to be in breach will want to self-investigate the value of any breach as early as possible to ensure they are not incorrectly penalized.

4. Bank Mellat

In June 2019, the UK settled a £1.25 billion (approximately $1.6 billion) lawsuit brought by Bank Mellat, an Iranian bank partly owned by the Iranian government, in relation to UK sanctions imposed against it between 2009 and 2013 due to alleged links to Iran's nuclear program. The bank claimed this led to losses of £3.2 billion (approximately $4 billion) due to its inability to do business in the UK financial sector and the substantial damage caused to its reputation in the UK and internationally. While details of the settlement were kept confidential, there was some press speculation that the settlement monies were transferred by the UK through a third country and entity, with U.S. sanctions concerns in mind. Bank Mellat continues to be sanctioned by the United States after its inclusion as a designated entity in October 2018.

The following Gibson Dunn lawyers assisted in preparing this client update: Judith Alison Lee, Adam Smith, Patrick Doris, Michael Walther, Stephanie Connor, Christopher Timura, Shruti Chandhok, Grace Chow, Cate Harding, Dyllan Lee, Allison Lewis, Jesse Melman,

R.L. Pratt, Tory Roberts, Richard Roeder, Samantha Sewall, Audi Syarief, Scott Toussaint, Brian Williamson, and Simon Woerrlein.

Gibson Dunn's lawyers are available to assist in addressing any questions you may have regarding the above developments. Please contact the Gibson Dunn lawyer with whom you usually work, the authors, or any of the following leaders and members of the firm's International Trade practice group:

United States:
Judith Alison Lee - Co-Chair, International Trade Practice, Washington, D.C. (+1 202-887-3591, jalee@gibsondunn.com)
Ronald Kirk - Co-Chair, International Trade Practice, Dallas (+1 214-698-3295, rkirk@gibsondunn.com)
Jose W. Fernandez - New York (+1 212-351-2376, jfernandez@gibsondunn.com)
Marcellus A. McRae - Los Angeles (+1 213-229-7675, mmcrae@gibsondunn.com)
Adam M. Smith - Washington, D.C. (+1 202-887-3547, asmith@gibsondunn.com)
Stephanie L. Connor - Washington, D.C. (+1 202-955-8586, sconnor@gibsondunn.com)
Christopher T. Timura - Washington, D.C. (+1 202-887-3690, ctimura@gibsondunn.com)
Ben K. Belair - Washington, D.C. (+1 202-887-3743, bbelair@gibsondunn.com)
Courtney M. Brown - Washington, D.C. (+1 202-955-8685, cmbrown@gibsondunn.com)
Laura R. Cole - Washington, D.C. (+1 202-887-3787, lcole@gibsondunn.com)
R.L. Pratt - Washington, D.C. (+1 202-887-3785, rpratt@gibsondunn.com)
Samantha Sewall - Washington, D.C. (+1 202-887-3509, ssewall@gibsondunn.com)
Audi K. Syarief - Washington, D.C. (+1 202-955-8266, asyarief@gibsondunn.com)
Scott R. Toussaint - Washington, D.C. (+1 202-887-3588, stoussaint@gibsondunn.com)

Europe:
Peter Alexiadis - Brussels (+32 2 554 72 00, palexiadis@gibsondunn.com)
Attila Borsos - Brussels (+32 2 554 72 10, aborsos@gibsondunn.com)
Nicolas Autet - Paris (+33 1 56 43 13 00, nautet@gibsondunn.com)
Patrick Doris - London (+44 (0)207 071 4276, pdoris@gibsondunn.com)
Sacha Harber-Kelly - London (+44 20 7071 4205, sharber-kelly@gibsondunn.com)
Penny Madden - London (+44 (0)20 7071 4226, pmadden@gibsondunn.com)
Shruti S. Chandhok - London (+44 (0)20 7071 4215, schandhok@gibsondunn.com)
Steve Melrose - London (+44 (0)20 7071 4219, smelrose@gibsondunn.com)
Benno Schwarz - Munich (+49 89 189 33 110, bschwarz@gibsondunn.com)
Michael Walther - Munich (+49 89 189 33-180, mwalther@gibsondunn.com)
Richard W. Roeder - Munich (+49 89 189 33-160, rroeder@gibsondunn.com)
Grace Chow - Singapore (+65 6507.3632, gchow@gibsondunn.com)

Related Capabilities

International Trade